RED HERRING THE BUSINESS OF TECHNOLOGY

EXHIBIT 3

Don't Call It Spyware

Companies that sneak software onto your computer say they are performing a legitimate service—and cleaning up their act.

February 6, 2006 Issue

Last year, 180solutions, a startup that calls itself a search marketing company, had its 15 minutes of fame. The six-year-old company, which says it had $53 million in revenue in 2004, ranked No. 7 on *Inc.*'s list of the 500 fastest-growing private companies in America.

It also made the cut on Deloitte & Touche's list of the 50 fastest-growing technology companies in the country, and CEO and co-founder Keith Smith was named to *Fortune Small Business*' Best Bosses of 2005 roster.

- ADVERTISEMENT -

Interact with Innovators.
Get 4 FREE Issues! - Subscribe Today!
RED HERRING
CLICK HERE

The adulation, however, horrified a significant sector of the technology industry—anti-spyware companies. Among them, Bellevue, Washington-based 180solutions has a murky reputation. Its software, the Zango Search Assistant, is classified by a number of companies, including Microsoft, CA, and Zone Labs, as "spyware," a term not likely to endear the company to most computer users.

180solutions vigorously disputes the tag—often with lawsuits—and says it has forced a number of its critics to back down. The company says it plays the role of matchmaker between users looking for hard-to-find content and the creators of content. During the process, 180solutions makes money by delivering ads tailored to user searches.

Content to Customers

It's a positive situation for all, says 180solutions' helmsman. Mr. Smith, 34, who once wanted to be a youth pastor, is onto his third startup with 180solutions. "We are creating a content economy," he says. "We are helping consumers get access to free content they would otherwise not have access to, and providing a platform to advertisers. It is about helping to monetize non-commercially relevant content."

The content could be videos, games, blogs, or even other software, all delivered quickly and easily, he says, in return for the privilege of inserting ads onto the user's computer. The controversy is about how the company installs its software, what it tells—and doesn't tell—users, and how difficult it is to remove the software.

180solutions says that 20 million people have Zango on their machines, and 5 million use it regularly every day to search the Internet. Mr. Smith says he doesn't get worked up over what security vendors say about his software unless their comments could hurt his business.

After a potential partner cancelled a deal because of the implications of being associated with a "spyware" company, 180solutions decided to do something drastic. Last November, the company sued Zone Labs, which makes the popular Zone Alarm firewall product, for calling its software spyware. Zone Labs was not the only one to disparage 180solutions' product in that way, but it was the "most egregious," says Mr. Smith. Zone Labs used terms like "malicious behavior" and "dangerous behavior" when classifying 180solutions' software, he says.

Zone Labs declined to answer specific questions relating to the lawsuit. The company, now owned by security giant Check Point Software, issued a statement saying it would vigorously defend its position. "We believe consumers have the right to know what programs reside on their computers, to understand what those programs are doing, and ultimately have the choice to keep or remove them from their systems," said Zone Labs. 180solutions' lawsuit has silenced many security companies and revived the debate on the nature of spyware and who should define it. It has also emboldened companies like Claria and WhenU, once known as "spyware" creators, to renew their drive for respectability. Backed by skyrocketing revenues and the lack of a clear standard in the security business on what really constitutes spyware, these companies are working to rebrand themselves and their product.

And it may be working. 180Solutions claims in a company blog that Zone Labs has modified its software since the lawsuit was filed. Formerly, Zone Labs warned users of "dangerous behavior" when it encountered a 180solutions program, but a newer security alert, the blog says, downgraded that to "suspicious behavior." Zone Labs declined to comment for this story.

'Parasites' No More?

The latest dispute between the anti-spyware vendors and the companies that are ostensibly protecting users from them highlights the changing world of spyware. Programs and tactics that were once considered a no-no are gaining legitimacy, creeping onto the desktop and finding big-brand advertisers to support them.

Consider Claria, a Redwood City, California-based company that was once loathed for its eWallet software. Today the company is a rising star. Last year, Microsoft was reported to be in talks with Claria about a possible acquisition. The rumors signaled a big step toward legitimacy for the company that once was the poster child for spyware. When Claria, formerly known as Gator, launched eWallet in 2000, it offered users a utility that would store address and credit card information computer users often had to type in. One click of a button and eWallet filled out online forms.

The software also started serving up ads and tracking the online behavior of users by embedding itself. Many users found eWallet annoying, and when they had difficulty getting rid of it, they filed a flurry of complaints against Claria.

That led to an investigation by the U.S. Federal Trade Commission and a lawsuit by a group of online publishers who called Claria a "parasite." But they couldn't stop the company from installing its software on millions of desktops and raking in revenues of $90 million and profits of $26 million in 2004.

Claria even filed for an IPO in April 2004 but negative publicity forced the company to withdraw the proposal four months later. An outcry from privacy experts also scuttled the Microsoft deal but Claria continues to serve high-profile clients such as Sony, Yahoo, and JP Morgan.

The difference is that the company has modified its product and is more upfront with users about its practices, says Scott Eagle, Claria's executive vice president and chief marketing officer. "We put our brand on the pop-ups so users would know why they were getting them," says Mr. Eagle. "We put our logo and a question mark on top of every ad so people who click on it could know why they were getting the ad."

Mr. Eagle declined to comment on talks with Microsoft but says the company's user base of 45 million is hard for anyone to ignore. And like 180solutions, he too talks enthusiastically about being part of a "content delivery revolution."

Anti-spyware crusaders like Sam Curry, vice president of eTrust Security Management, a unit at CA, say companies like Claria, 180solutions, and New York City-based WhenU are making their business models appear more innocent than they really are. The goal of these companies, he says, is to get the biggest installed base of users and the way they do that is by removing control from the user.

"For these companies, the end user isn't their customer," says Mr. Curry. "The customer is the advertising company placing the ads. The product they deliver is the end user." And to do that they use tactics that don't add up on the scorecard security companies like CA have created to define spyware, says Mr. Curry.

Adware or Spyware?

That raises a fundamental question about the definition of spyware. The generally accepted standard in the security industry is a program that is invasive, installs itself surreptitiously on a user's computer, and does not give the user a fair chance to remove the program.

180solutions and Claria say they don't do any of that. So they are trying hard to make users familiar with another term—adware, a label they detest as much as spyware but say is closer to describing what their software does. Apparently, there's a difference between the two. Adware companies only want users who want to have their software on the computers. The spyware guys install their stuff everywhere.

Adware is different from spyware because it gives users greater degree of control and is more respectful of their rights, agrees David Cole, director of Symantec's Security Response Center. Still, the distinction can be fuzzy, he says. It all comes down to the degree of transparency, privacy, and control that a program gives its users.

Even that is easier said than done. Claria and 180solutions say their software tells users exactly what it does, what they can expect from it, and how they can uninstall the program. Security experts aren't so sure. They say that even the so-called legitimate adware companies hide behind long license agreements that few users take the time or effort to read. "In my opinion we need the equivalent of the food label for software—tell a user in a consistent, easy-to-understand format what the software will install, and what information is sent back out," says Doug Camplejohn, CEO and founder of Mi5 Networks, a Sunnyvale, California-based startup that makes anti-spyware appliances for enterprises.

Sometimes, adware companies let affiliates do the canvassing and installation of the programs, thereby denying any direct association with privacy violations, say experts. Claria and 180solutions say they are cleaning up their distribution network. 180solutions says it has even sued former distributors for installing their software on users' computers without proper consent.

Going Legit

However, it will be a while before the industry can accept such companies as legitimate players, says Mr. Eagle. He compares the treatment of adware today as similar to what antivirus companies did to tracking cookies a few years ago, when most of them listed the cookies as dangerous to a user. Now they are accepted by everyone. Someday adware will get the same respect, he says.

But to win that legitimacy, adware companies need to get past gatekeepers like CA and Symantec, which have accelerated their efforts to define a standard for the industry on ranking programs as spyware. These companies, along with their industry peers, consumer protection groups, and privacy experts, set up The Anti-Spyware Coalition in June 2005.

Last month the coalition released a final working report that outlines the rules for dealing with false positives, disputes over classification, and a risk model that will lay out the different levels of dangers posed by various kinds of spyware products. "The market is maturing so we need to be able to paint in finer strokes," says Symantec's Mr. Cole. "It's no longer just about good or bad, it's about varying risk levels and the consumer appetite for risk."

Instead of security companies, it is the spyware and adware makers who are laying down the rules now, says Ari Schwartz, associate director of the Center for Democracy and Technology, which runs the coalition. "They have been trying to divide and conquer till now," says Mr. Schwartz. He believes a clearly defined standard will put power back into the hands of the security vendors.

Claria and 180solutions say they welcome the initiative and have been working to clean up their act. Ultimately, it will be about the value they can offer their users, who will then decide whether to keep adware or spyware software on their computers. 180solutions says lawsuits can only take it so far. Meanwhile, it is ready to do what it takes to gain acceptance. "There haven't been a lot of rules around what is OK and what is not OK," says Mr. Smith.

Until it finds that balance, 180solutions is likely to keep its lawyers busy.

© 1993-2006 Red Herring, Inc. All rights reserved.

180 Solutions Code of Conduct- Can They Make it Work?

by Wayne Porter

180solutions Code of Conduct

Extract Courtesy of 180solutions.

Date: 05.01.2005

Recently 180solutions, an adware company struggling with getting their rogue affiliates under control, took the time to share with us their Code of Conduct for distributors. The question looming on everyone's mind is can 180solutions reign in their rogue distributors and enforce their terms against distributors engaging in unsavory distribution practices?

Extract: 180solutions Code of Conduct

Distributor agrees to accurately provide easy to read and understand notice and information to all end users of 180solutions products and all other applications that are bundled with 180solutions products before both initiating a download to and installing the products or applications on an end user's computer, and to give such end user an easy and appropriate method to agree or not to agree to such installation.

Distributor shall under no circumstances attempt to launch a 180solutions product executable without first displaying the above-described messaging and receiving explicit user consent for the installation. 180solutions reserves the right to approve final wording of this messaging and to require periodic changes as necessitated by changes to 180solutions products or for other business reasons. In addition, each installation of 180solutions products by Distributor must include and be subject to the then current 180solutions End User License Agreement (EULA).

Distributor will ensure that the end user may easily remove/uninstall not just the 180solutions products, but each and every other application bundled with 180solutions products by using the Microsoft Windows Add/Remove Programs menu. Distributor will also ensure that all applications bundled with 180solutions products adhere to terms no less restrictive than those contained in this Agreement follow these same codes of conduct. Other products or applications that act as program

You just clicked AGREE, but do you know what that End User License Agreement says?

Analyze Your EULA

Help with the BUST!

Become A Spyspotter!
Bust the Bad Guys!
Click here and give us what details you have and let our international research team take it from there. If you desire your report will remain anonymous.

Recent Blog Posts

- Skype Worm Variant Targets Other Instant Messaging Clients
- The Podo Hijack, and an Empty Sweetbox...
- A Korean Trick or Treat?
- Skype Phish?
- Ben Edelman On InfoWorld
- USB Worm Targets Firefox, Orkut and YouTube
- TV Hacking...
- Images Speak Louder Than Words
- Pictures From An Exhibition
- First ID Number Spoofing Attacks Against Popular Twitter

Recent Modifications

2007-5-30 Troj/Agent-CL
2007-5-30 WinAntiVirus
2007-5-30 SpyWare Secure
2007-5-30 CoolWebSearch
2007-5-30 CurePCSolution
2007-5-29 Agent-ECM
2007-5-29 Zone-DL.Plugin
2007-5-29 PWSLegMir
2007-5-25 About Blank
2007-5-24 Trojan.Win32.sky

"Trojans" (installing additional applications without full product descriptions and EULA acceptance) shall not be bundled with any 180solutions product.

At any time, 180solutions will be allowed to test all products with which a 180solutions product is bundled to ensure Distributor's compliance with the guidelines and terms herein. Neither the conducting of such testing, nor the failure to do so, will act as any certification or other affirmation that Distributor is in compliance with the terms and conditions herein nor relieve Distributor from any liability hereunder

Distributor is responsible for the actions of its partners and affiliates and will ensure that each partner and affiliate agree in writing to terms and conditions no less restrictive than those contained herein, and that appropriate messaging and EULA acceptance precedes every installation of a 180solutions product or another product that is bundled with a 180solutions product. (1) If Distributor discovers a partner or affiliate (either direct or indirect) is in violation of any of the terms and conditions of this Agreement, then Distributor agrees to immediately call such action to the attention of 180solutions and to immediately terminate its distribution relationship with such partner or affiliate. In addition, Distributor shall be subject to liquidated damages as set forth in the immediately following paragraph. (2) If 180solutions discovers independently that Distributor or one of its partners or affiliates (either direct or indirect) is in violation of any of the terms and conditions of this Agreement, then 180solutions shall immediately notify Distributor and Distributor agrees that it will immediately terminate its distribution relationship with such partner or affiliate. In addition, Distributor shall be subject to liquidated damages as set forth in the immediately following paragraph.

The parties agree that strict compliance with the terms and conditions of this Agreement is at the essence of the relationship between Distributor and 180solutions, Inc. The parties further agree that damages from breach of this Agreement may be difficult to calculate at the time of any breach. Accordingly, the parties agree, in addition to any indemnification obligations herein, to liquidated damages: (a) in the case of (1) above, equal to the amount paid by 180solutions to Distributor relating to the breach by Distributor, its partner or affiliate, and (b) in the case of (2) above, equal to two times (2x) the amount paid by 180solutions to Distributor relating to the breach by Distributor, its partner or affiliate.

If any claim is made, or any action or proceeding is instituted, against 180solutions that alleges or is based upon or arises out of Distributor's breach of any representation, warranty or obligation arising under this Agreement, Distributor shall indemnify and hold 180solutions harmless from all damages, awards, costs and expenses (including reasonable attorney fees) associated therewith.

For purposes of this Agreement, a "bundled" product or application includes all other products or applications which may be downloaded to, and installed on, the end user's computer at the same or at a later time by an application or product delivered at the same time as the 180solutions product, excluding new version updates and upgrades to the initially delivered application or product.

Our Take on 180's Code of Conduct

We think it is a good step that 180solutions has provided a Code of Conduct for their distributors, but Codes of Conduct are no guarantee that people will get a fair shake. Time will tell if 180solutions can get a handle on their distributor base and reign in the unscrupulous distributors taking advantage of browser exploits, security holes, and deceptive installations. It all boils down to action and not words.

For more information see the interview we did with AdBumb, an advertising newsletter, about the distribution problems with 180solutions and some of 180's own responses.

Unless otherwise noted this article is Copyright © 2007 by FaceTime Communications, Inc. This article may not be resold, reprinted, or redistributed for compensation of any kind without prior written permission from FaceTime Communications, Inc. For reprint or media inquires please contact us with the phrase "Spyware Guide Articles" in the subject line and we will by happy to assist you. Links to this article from other websites are appreciated and encouraged. Users are also encouraged to utilize our RSS system to provide unique content and extracts for their site.

Related Articles

- Anatomy of a Drive-By Install- Even on Firefox
- Adware Self Regulation- Not The Answer

Read other articles (back to full list)

Spyware Remover Download
Remove Spyware, Adware, Trojans & Keyboard Loggers. Rated 5 Stars!
www.pctools.com

Which Spyware Remover?
Don't download any free Spyware remover until you read this article
www.CompareSpywareRemovers.or

Top 2007 Spyware Removers
Compare and Download the 5 Top 2007 Spyware Removers for Free.
SpywareRemoversReviewed.com

Antivirus For Gamers
An AntiVirus-AntiSpyware that won't Interrupt your game! Free Scan Now
www.Stop-Sign.com

Ads by Google

© Copyright 2006, FaceTime Communications, Inc. All rights reserved.

67 of 155

SunbeltBLOG

A blog about activities, products and ideas at Sunbelt Software, one of the leading developers of security software to protect against spyware, spam and

FRIDAY, FEBRUARY 24, 2006

180Solutions issues mea culpa

We'd like to bring readers up to date about the illegal force-install of 180solutions' Zango Search Suite software that Ben Edelman documented on Monday.

As we noted late Monday, 180solutions issued a press release in which the company claimed to have identified and shut down the perpetrator of the force-install documented by Edelman. 180solutions also claimed to have "re-messaged" all the victims of that particular force-install.

From 180solutions' press release:

> "Despite an unprecedented effort by some industry critics to keep secret the critical information that would have led to a quicker shutdown of the fraudulent behavior, the company, through its own policing mechanisms, was able to track down the nefarious actor responsible and shut him down. This rogue publisher will not receive any payment for these installs and as stated in the Code of Conduct, will be subject to further financial penalties and legal action ... While a non-trivial software hack was used in this instance to subvert the consent process, the S3 functionality enabled the company to go back and re-message every user who received its software from "Sniper84" and provide them a one-click uninstall."

As it turns out, the claims made in this press release were innacurate. When 180 issued the press release, 180 had not yet shut down the perpetrator of the illegal force-installs documented by Edelman, and 180 had not yet re-messaged the victims. 180solutions had managed to shut down someone going by the online name of "Sniper84" for violations of the ZangoCash affiliate agreement, but Sniper84 was not the party responsible for the bad installs documented by Edelman.

They have issued a blog posting, entitled "Mea culpa":

> On Monday, we announced we had shut down a hacker responsible for forcibly installing our software. Those forcible installs were done without our authorization and were contrary to our policies. At the time, we believed this was the same individual Ben Edelman had (cryptically) described, but purposefully not fully identified, in a post to his website earlier that same day.
>
> As it turns out, we didn't get Mr. Edelman's guy on Monday. The guy we got on Monday, Sniper84, was also installing our software in the same unauthorized manner. The hacker Mr. Edelman discovered, csk2000, was shut down early Tuesday afternoon after we were finally able to identify him in the course of our ongoing investigative efforts. (Security researchers at Sunbelt Software have since confirmed that we found the "correct" culprit on Tuesday.)

So only later — sometime on Tuesday or early Wednesday did 180 finally manage to shut down the true perpetrator of the exploit-driven installs Edelman found.

How do we know this?

Well apart from 180's blog posting, it had struck us as odd that 180 would have managed to identify and shut down the party responsible for the installs discovered by Edelman so soon. 180's press release came within hours of Edelman's own report, and Edelman had purposefully not identified the web site at which the exploits were being performed. Moreover, Sunbelt's own investigation had turned up nothing to point to any person going by "Sniper84." How could 180 figure out this puzzle so quickly? If 180 could figure this out substantially on its own, why had 180 needed Edelman's initial report in order to take action here.

Also puzzling was the fact that our infested machines had not been "re-messaged" with a "re-opt-in" box and "one-click uninstall," as 180 claimed had been done for victims of the rogue installs. We browsed on multiple test machines, but we never got this prompt, and neither did Edelman.

A Sunbelt researcher re-staged the exploit on Tuesday morning, confirming that the perpetrator's 180 installation files still worked as usual. This fact is revealing, because 180's installation system lets 180 halt installation by distributors who have been ejected from 180's distributions program. If 180 had actually managed to shut down the perpetrator of the installs documented by Edelman, as 180 claimed Monday, the Zango installer used in those exploits would not have worked on Tuesday. But it did.

On Wednesday we continued to monitor our test machines. Late afternoon on Wednesday one of Sunbelt's researchers again re-staged the exploit with the Zango installer used by the perpetrator. This time, the installation of Zango software was stopped in its tracks, telling us that 180 had finally managed to shut down the right perpetrator.

We asked Ben Edelman how 180 could so quickly have identified the perpetrator of the force-installs he documented, especially since Edelman had not disclosed the web site where he found those installs. Edelman pointed to his video which, though scrubbed clean of any info identifying the site, did contain one key bit of data: the extraordinary speed with which the S3 consent box had been dismissed by the exploit software. That bit of data could be used, Edelman noted, to single out these nonconsensual installs in 180's logs and database: Just look for programs installed less than one second after users were (purportedly) asked for permission. Comments made by 180 spokesperson Sean Sundwall to eWeek seem to confirm Edelman's suspicion:

> 180 would have spotted the illegal installs earlier, but lacks an integrated system for monitoring telltale signs of rogue behavior, like an unusually high rate of user acceptance of the 180 software (the rate is typically between 5 and 10 percent), or an unusually rapid consent to the license agreement, Sundwall said.

So, although 180 did eventually identify the perpetrator responsible for the illegal force-installs documented by Edelman, they had not shut down that rogue distributor by Monday, as they incorrectly claimed in their press release. Instead, 180 wouldn't actually shut down this installer until sometime Tuesday or Wednesday (the time between our two re-tests of the Zango installer used in the exploit-installs).

Needless to say, this episode points out that the much-ballyhooed S3 technology is not sufficient to block "rogue" distributors. 180's S3 technology failed to guarantee that users would always have to consent to the installation of 180's software (as 180 claimed it would) and 180 failed to shut down the perpetrator responsible for the rogue installs exposed by Edelman before it rushed out its press release on Monday.

We are satisfied that the perpetrator of these rogue installs has been shut down. But 180's S3 technology has turned out to be far less robust and effective in combating rogue distributors than 180 would have internet users believe.

Eric Howes
Director of Malware Research
Sunbelt Sofware

POSTED BY SUNBELT SOFTWARE BLOG AT 12:34 PM PERMALINK

COMMENTS (3) | TRACKBACK (0)

<< Home

180solutions / Doll Idol - Critiquing 180solutions's Response

180solutions's Misleading Installation Methods - Doll Idol - Ben Edelman

On January 9, 2006, I posted 180solutions's Misleading Installation Methods - Doll Idol, analyzing current 180solutions "S3" installation practices. 180's Sean Sundwall subsequently posted a response (at ZDNet and at Vital Security). This page critiques each point of 180's response.

[Targeting Kids | Off-Screen Footer without Scroll Bar | Failure to Disclose that 180 Shows "Pop-Ups" | Failure to Disclose Privacy Effects | Misleading and Missing Buttons in Installation Confirmation Window | Discouraging Removal]

Targeting Kids

I claimed that 180 is "promot[ed] at sites targeted at children."

Sean responded that it is "patently false" that Dollidol is a child's site. Sean says "Dollidol.com is not targeted at kids, period."

I think Doll Idol's content (avatars in the style of barbie dolls) largely speaks for itself.

MSNDOLLZ.COM
1000'S OF MSN AVATARS TO CHOOSE FROM...
Banner Image from the Dollidol Site

Some pages of the Doll Idol site specifically describe associations with children (e.g. the "school" category of avatars, listing ages as low as "first grade"). The rest of Doll Idol is consistently designed in a playful childlike style, featuring numerous pictures of teenage (or younger) girls.

Readers should visit Dollidol.com and draw their own conclusions as to its apparent audience.

Sean continued: "Suggesting that a site is targeted at children because it has animated characters is a bit naïve."

I disagree. It's not "naïve" to think a site targets kids when that site includes animated characters. To the contrary, longstanding FTC COPPA regulations specifically instruct considering the presence of animated characters when evaluating whether a web site is directed to children. See also FTC Rule 16 CFR Part 312, provision 312.2, defining sites "directed to children."

An Image from the Dollidol Site

Beyond the presence of animated characters, the FTC's regulations also call for evaluation of a site's subject matter. Dollidol.com repeatedly references "dolls," including in the site's title and in its domain name. These many prominent refernces weigh towards a finding that the Dollidol site is targeted at kids.

The FTC's regulations further call for assessment of the age of any models pictured on a web site. Dollidol's sketches show young women who are distinctively young-looking. (See e.g. images above.) A mere 30 pixels below Dollidol's links to install 180solutions, Dollidol includes a prominent "put your photo on an avatar" feature with a photograph of a girl. See image at right. I estimate the model to be ten years old. The young age of the models pictured in Dollidol's sketches and photographs also indicates that the Dollidol site is targeted at kids.

Off-Screen Footer without Scroll Bar

return to top

I claimed that 180 "disclos[es] the presence of bundled 180solutions advertising software in an off-screen footer without scroll bars."

Sean responded that "When you have a screen resolution of 800x600, there are a lot of things you're going to have to move around to see properly. ... Judging our business practices on an ancient screen resolution shows desperation."

Certainly users with bigger screens will see the 180 disclosure at issue (deficient as that disclosure's substance may be, per subsequent discussion). I never said anything to the contrary.

But 180's duty to disclose -- to provide appropriate information, so that users know what they're getting -- is a duty that applies to *all* users, not just to users who happen to own the latest computer technology. Sean and I are fortunate to have high-resolution screens where we can see large web pages as they were intended. But ordinary users shouldn't be tricked into installing 180 just because they have older PCs. And since extra software is particularly harmful to old PCs -- which are likely to be slowed more by nonessential programs running in the background -- I'm actually *particularly* concerned about unwanted 180solutions installations on such computers.

I'm hardly the first to point out the need to provide appropriate disclosures even to users with older computer technology. See the FTC's 2000 "Dot Com Disclosures," which specifically warns advertisers "Don't ignore technological limitations" (section 1.c.i.) when providing disclosures.

Failure to Disclose that 180 Shows "Pop-Ups"

return to top

I claimed that 180 "fail[s] to disclose that 180's ads are shown in pop-ups."

Sean responded that "We will be changing the language in our plain-language disclosure to better address the types of ads we serve."

I applaud this change. If users are told that 180 will show "pop-up ads," users will be better able to assess whether 180 is a program they want on their PCs.

I pointed out that 180's disclosures fall short of requirements of TRUSTe's Trusted Download program.

Sean adds that TRUSTe's software download standards are "not yet a standard," therefore not binding on 180.

I agree, but that's irrelevant. 180 has a preexisting duty to disclose material effects of its software. Here again, see the FTC's "Dot Com Disclosures," which require that "material information" be disclosed "clear[ly] and conspicuous[ly" before a user enters into a transaction. Under FTC rules, material information is information likely to affect a consumer's conduct with respect to an offer.

Since users are known to hate pop-up ads, reasonable consumers are less likely to install software that shows "pop-ups" rather than ordinary "advertisements" (e.g. within a program window). So this characteristic of 180's software is material. As such, under existing FTC rules, 180 must disclose that its ads will appear in pop-ups.

Failure to Disclose Privacy Effects

return to top

I claimed that 180 "fail[s] to disclose the privacy consequences of installing 180's software." I described 180's privacy effects as "track[ing] what web sites users visit and ... send[ing] this information to 180's main servers."

In response, Sean claimed that "180solutions does not 'track what web sites users visit and ... send this information to 180's main servers.'"

Sean's claim is false. 180 absolutely *does* track what web sites users visit.

In 2004, I posted a packet log showing a 180solutions transmission of the specific URL I visited on a test PC. (I have continued to observe near-identical transmissions from 180solutions software through the present day.) Copying here for readers' convenience:

```
GET /showme.aspx?keyword=delta.com&did=762&ver=5.9
&duid=531byhiprtvdgvadrfmfcgtxxyrjmg&partner_id=195252523
&product_id=762&browser_ok=y&rnd=21&basename=zango
```

keyword trigger

user id

&tzbias=5&MT=8C5F0B5F1538C31DC2F456CC736BC33B268398A0
&DMT=8C5F0B5F1538C31DC2F456CC736BC33B268398A0&bid=0&SID=ANCVAXYV
&OS=5.1.2600.2&SLID=1033&ULID=1033&TLOC=1033&ACP=1252&OCP=437
&DB=iexplore.exe&IEV=6.0.2800.1&TPM=200785920&APM=41066496
&TVM=2147352576&AVM=2006102016&FDS=1834094592&LAD=1601:1:1:0:0:0&WE=5

The yellow highlighting (above) shows that 180 *does* track what web sites users visit. In the example above, 180 tracked and transmitted the fact that I was browsing the www.delta.com web site.

Sean's response cloaks 180's tracking in a variety of euphemisms -- "we parse the URL string for keywords" and "send[] a request to our servers." Whatever complicated language Sean chooses to describe 180's behavior, my initial article describes 180's practices with appropriate clarity: 180 tracks what web sites users visit.

Sean further commented that "As far as privacy concerns, I'm not sure what they are."

I'm surprised that the head of communications for a major "adware" vendor is "not sure" about the privacy concerns associated with his employer's software. Sean might prefer not to discuss these consequences. But the consequences are real and, for many users, serious.

As described above, 180 tracks what web sites users visit. Users have good reason to be concerned about these transmissions. Even a partial list of users' web site visits and search terms can be extremely revealing, capturing detailed and sensitive information. When I last reviewed 180's ad target list, I saw tracking of the most sensitive of web sites -- not just financial sites (like banks and credit card sites) but job search sites (jobs.com, hotjobs.com, etc.) and even health sites (aids.org, aidsaction.org, breastcancer.org, etc.). Reasonable users may not want 180 to know that they're visiting such sites. And while 180 may not know users' names, 180 does assign each user a distinct ID code (green highlighting above). These ID codes allow after-the-fact searching if 180 so chooses -- or if subpoenas or other proceedings demand such information.

Misleading and Missing Buttons in Installation Confirmation Window

return to top

Referring to 180's use of the word "finish" to *start* an installation users had never requested, I claimed that 180 "us[es] misleading button labels to encourage installation."

Sean responded: "There is no trickery here unless you believe today's average computer user doesn't understand the word 'cancel.'"

The question at hand is not whether the "cancel" button is properly labeled. The question is whether the affirmative button, "Finish," is appropriate under the circumstances. My claim is that it is inappropriate to label a button "Finish" when that button *starts* a process a user had not previously requested. "Finish" suggests that the user had already agreed, that this final step is insubstantial and unimportant, and that important actions are already complete. In contrast, a label like "Accept installation" or "I agree" would tell a user, appropriately, that nothing has been done yet, that no permission has been granted yet, and that it's not too late to deny permission.

Sean says that my analysis "insults the intelligence of the increasingly savvy computer user."

I disagree. Savvy users may be able to figure out that 180's S3 screen is seeking permission to install software on their computers. But I'm concerned about more than just savvy users. I'm equally concerned about newbies, about kids, about confused users, and about users who are in a hurry.

180 distributes its software on mass-market web sites catering to ordinary users, and its installation procedures shouldn't only be accessible to experts. Instead, 180 should aspire to be as clear as possible as to what they seek to do, how, and why. Appropriate, accurate, clear language can assist users in quickly understanding and assessing 180's offer.

I claimed that 180 "hid[es] standard Windows buttons to hinder cancellation of installation."

Sean responded: "There are countless examples of reputable installation screens that do not have the "x" in the upper right hand corner. I get one from my Palm software every time I reboot my computer."

Certainly some programs properly display windows without "x" buttons. But I'm not sure that an "x"-less window is appropriate for an installation confirmation screen window. (And since Palm software is already installed on Sean's computer, I don't think his Palm windows are a good example of the "reputable installation screens" Sean claims lack "x" buttons.)

Official safe browsing tips (from the computer industry and even from the US government) specifically instruct users to press "x" in any unrequested popup, to reduce risk of installing software accidentally. By intentionally hiding this "x" button, 180 specifically blocks this industry-standard and government-endorsed method for users to protect themselves.

In 180's S3 installation box, the "x" button would perform the same function as pressing "cancel." Whatever the practices of other vendors, 180 should add this button to its windows, to give users an additional way to decline 180's offer.

Discouraging Removal

return to top

I claimed that 180 "discourag[es] removal with false warnings of risks to other applications." I pointed out that 180 prominently says "uninstalling Zango will disable any Zango-based applications or tools on your computer," even when 180 knows that no such applications or tools have been installed.

Sean responded that "we do discourage uninstallation of our software but we do it without trickery and without fearmongering."

As an advertising technology company, 180 boasts of its "highly targeted" ads, which specifically respond to exactly what a user is doing online. But when it comes to 180's uninstaller, 180 is far less sophisticated. In particular, 180 shows its broad "will disable any Zango-based applications" whether or not any such applications have actually been installed. For users with no such applications -- users who received 180 at a site like Doll Idol -- this messaging is simply *false*. Whether or not this false statement amounts to "trickery" or "fearmongering," it improperly warns Doll Idol users about a problem they're certain not to face. In my view, this statement is misleading as to Doll Idol users, and it therefore should not be included in 180's uninstaller.

Telling users about the *real* negative effects of removing 180 is one thing. Making up effects they won't actually face is quite another.

MediaPostPublications HOME • CLASSIFIEDS • MANAGE SUBSCRIPTIONS • COMMUNITY • EVENTS • MEDIA KIT • HELP

Teens? Gen Xers? Online every day?
Free Report
Casale
Advertising Online Is Better Here

SEARCH Advanced Search Archives

Home > All Archives > Online Media Daily Archives > Tuesday, Jan 24, 2006 Welcome | sign-out Thu, May 31, 2007

EMAIL THIS ARTICLE PRINT REPLY SUBSCRIBE TODAY'S EDITION

Watchdog Asks FTC To Sue 180solutions

by Wendy Davis, Tuesday, Jan 24, 2006 6:00 AM ET

AFTER TWO YEARS OF ATTEMPTS to work with adware company 180solutions, the nonprofit watchdog Center for Democracy and Technology Monday filed a complaint against the company, charging that it engages in "distribution practices that appear to be broadly unethical and in many cases, illegal."

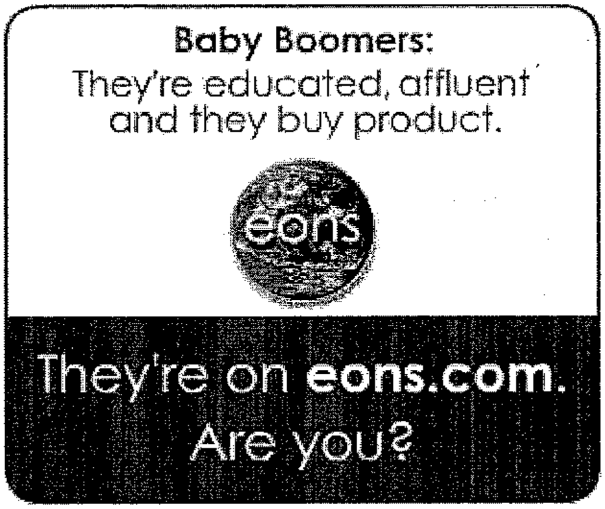
In a 91-page document filed with the Federal Trade Commission, the Center for Democracy and Technology, or CDT, alleged that 180solutions' "core business model depends on third-party affiliates committing unfair and deceptive practices on the company's behalf."

"Despite CDT's reports, audits from the company's own consultants, and public reports from security experts, 180solutions has remained brazenly reckless in its efforts to get its software on users' computers," reads the complaint, which asks the FTC to seek monetary damages against 180solutions and an injunction banning the company from the unfair and or deceptive installations of adware.

180solutions responded with a statement that it had voluntarily "made improvements to address every reasonable concern that the CDT has made us aware of."

The complaint filed Monday--and comments made by representatives of the CDT--made plain the group's frustration with 180solutions, despite the company's aggressive and public attempts to improve its image.

"To have this continually happen is really beyond the pale of what a responsible software company should be doing today," CDT Deputy Director Ari Schwartz said in a conference call with reporters Monday morning. The CDT also plans to speak with



Today's Most Read

1. Agency of the Year: Editor's Letter
2. Standard, Flash, or Rich Media Expandable Banner Finalists
3. What Happens When You Let Go
4. In-Banner Video Finalists
5. The Big Spenders

180solutions' advertisers, and inform them that they are affiliated with practices that result in allegedly improper adware installations.

The CDT's papers detailed a litany of examples of 180solutions' ad-serving software being installed without adequate notice to consumers. The CDT also stated that it made numerous attempts to work collaboratively with 180solutions, but that improper installations continue to occur. The most recent example cited in the complaint occurred on Jan. 6, when 180solutions' adware allegedly was installed without users' permission through a worm in America Online's instant messenger.

In the last year, 180solutions has tried to burnish its image by publicly distancing itself from companies accused of using improper installation methods; in some cases, 180solutions filed lawsuits against former affiliates that allegedly installed adware without first obtaining consumers' consent. 180solutions also recently sued a software removal company for "trade libel" for classifying 180solutions' ad-serving program as "spyware."

In a Dec. 29 post on the 180solutions blog, Sean Sundwall, director of corporate communications, boasted that 180solutions had undertaken "a complete overhaul of our distribution model." By the end of October, according to the blog post, 180solutions had stopped using third-party distributors--which it defined as "partners of partners."

Currently, 180solutions contracts directly with about 1,000 Web companies that distribute its software. One of those, CJB.net, also was targeted Monday by the Center for Democracy and Technology.

Despite its recent steps, 180solutions continues to have a poor reputation among watchdogs. Eric Howes, a spyware researcher and director of malware research at Sunbelt Software, collected and posted a list of examples of allegedly improper installations on the site SpywareWarrior.com; his research was cited by the CDT in its complaint.

The basic problem, according to Howes and the CDT, is that 180solutions' business model relies on partners to distribute its ad-serving software. 180solutions has stated in the past that companies have no financial incentive to improperly install adware; 180 also maintains that it doesn't profit from improper installations because consumers quickly remove unwanted software.

But others say that not all consumers are technically savvy enough to immediately remove the programs. Even if the adware remains for just a few days, that's long enough for 180solutions to serve at least some impressions.

"Until they change their business model, the problems will continue," Howes said.

A spokesman for the CDT agreed: "Their business model created a situation where bad installations are happening," said CDT spokesman David McGuire. "They can't just wash their hands of their own network."

Recent Online Media Daily Articles

Social Nets Rise Rapidly in U.K. May 30, 6:00 AM
Social networks were the big U.K. gainers in comScore's April World Metrix ratings. Bebo, the subject...

Huffington's New Sections More Ad-Friendly May 30, 6:00 AM
The Huffington Post's expansion of its coverage into five new sections, combined with a "cleaner, less...

MindShare Interactive Names Digitas Exec As New EVP May 30, 6:00 AM
Former Digitas executive Huard Smith joined MindShare Interactive Campaigns as its new executive vice president. The...

Knitting Factory, ShopText Deliver Concert Tickets Via Text May 30, 6:00 AM
Live music fans in New York City and Los Angeles can now "text-to-purchase" tickets to concerts...

ABC News, Heavy.com & AOL Turn To CGM May 30, 6:00 AM
Several new announcements illustrate how media companies are increasingly relying on consumer-generated media (CGM) to flesh...

Agency.com Names Jordan Warren To Lead SF Office May 30, 6:00 AM
Omnicom's agency.com named online marketing pioneer Jordan Warren as president of its San Francisco office, filling...

FTC Investigation Into Google/ DoubleClick: Boom or Bust? May 30, 6:00 AM
The Federal Trade Commission's preliminary investigation into the Google/DoubleClick deal has more to do with marketplace...

Skybus To Be First Airline To Take Ads On Web Site May 30, 6:00 AM
Columbus, Ohio-based discount air carrier Skybus is looking to derive ancillary revenue from all sources. It...

NBC Digital Under New Management May 30, 6:00 AM
The digital end of NBC Entertainment came under new management Tuesday with the appointment of Ben...

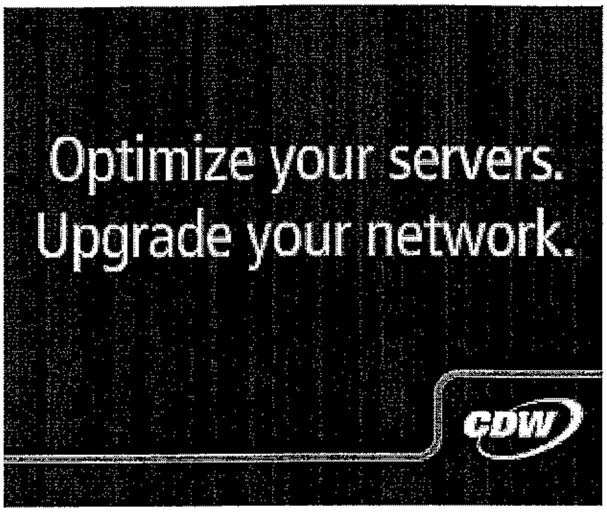
Digicorp Inserts Ads Into Media Files, And Follows Them Everywhere May 29, 6:00 AM
Putting a new twist into the hot category of in-stream advertising, Digicorp, Inc. has launched a...

>> Online Media Daily Archives

ABOUT MEDIAPOST • MEDIA KIT • RSS FEEDS • PRIVACY • TERMS & CONDITIONS

MediaPost ©2007 MediaPost Communications. All rights reserved.
1140 Broadway, 4th Floor, New York, NY 10001
tel. 212-204-2000, fax 212-204-2038, feedback@mediapost.com

ads powered by atlas.


Optimize your servers.
Upgrade your network.
CDW

REALTECHNEWS
Independent Tech

Search

search...

Search

- Home
- About
- Archives
- Free Magazines
- Tech Jobs

· Ads by Google· WB TV The WB ABC Family One Tree Hill

Previous entries
Next entries

May 10th, 2006

Warner Bros Partners with 180Solutions

By Jimmy Daniels
Contributing Writer, RealTechNews

In one of those moves you just have to shake your head at, Warner Bros has partnered with 180Solutions to distribute shows made exclusively for the web. The plan is to add a third show, and to use other models to distribute the shows, such as on Sprint telephones and BitTorrent.

> So far, 180solutions has made three episodes of "Deception" available on Zango.com, as well as on about 50 sites within its publisher network, Baur said. Each episode of "Deception," starring "Days of Our Lives" veteran Roark Critchlow and produced by his production company, lasts between three and five minutes. The series is aimed at women between the ages 35 and 54, and will contain 30 episodes total, with new episodes appearing on Monday, Wednesday, and Friday. "Medical Island," aimed at males 18 to 24, will consist of 10 episodes total. 180solutions will have exclusive Web rights to distribute the shows for 120 days.
>
> Warner Bros. and 180solutions have been quietly working together for almost a year, mainly in the gaming space, but the relationship had been kept under wraps. *Source: Mediapost via Todd Crawford*

They have also signed a deal with BitTorrent to distribute the shows, pricing for the service has also not been announced but sources reveal that television shows might cost as little as $1 while films might cost around the same amount as DVDs.

We Say: Apparently, they have been working with 180Soultions for about a year, mainly in the gaming space, not sure what that means yet, but I will be looking closer at their site to see if they are actually distributing the software for 180 or if 180 is distributing Warner Bros games to kids with the adware installed. This is where we, as consumers need to start boycotting companies that actually partner with adware and spyware companies, like Warner Bros., they are funding the adware model. Companies like Warner Bros may as well distribute the adware themselves. So, now we can either pay for their shows, or get free crap with their crap. Looks like they are shutting down their message boards, although some posts have May 1st dates, the only email I could find so far is legal@wb.com and privacy@wb.com. Email them and let them know what you think of 180Solutions and their practices. We have to start somewhere and it may as well be Warner Bros we send a message to.

Share and Enjoy: These icons link to social bookmarking sites where readers can share and discover new web pages.

Kill 180 Search Assistant
SpywareBot Destroys 180 Search 5 Star Rated - Download 100% Free!

Remove 180Search Hijacker
Complete Removal of 180 Search. Solution that Works! Free Download.

Ads by Google

You can leave a comment, or trackback from your own site. RSS 2.0

16 comments to "Warner Bros Partners with 180Solutions"

1. Mart says:

   You would think that they would stop themselves from doin g this after the Sony Rootkit mess.

   May 10th, 2006 at 2:03 pm

2. David Johnston says:

   Why did they choose to partner with 180Solutions, of all companies? I'm fine watching ads during a TV show, but I don't want ad-delivering software or spyware put on my machine. That seems to be the only thing 180Solutions does though, so I'm not looking forward to this.

   May 10th, 2006 at 2:53 pm

3. JR says:

   "Funding the adware model?" Welcome to the 21st century - or maybe you are still in the 20th century - adware is what made network TV free for the last 70 or so years, and if you don't like the ads, then you turn off the TV and read a book. At least now, thanks to the 1-to-1 nature of the Internet, the entertainment and the advertising (adware) that supports it can both be more relevant and tailored to the individual. Spyware is a different matter altogether, but I don't see that in this deal.

   Boycotting ad-supported entertainment is like the buggy-makers thumbing their noses at Ford. Totally out of touch with where the world is going.

May 10th, 2006 at 3:22 pm

4. Jimmy says:

   JR, please, 180Soultions is not the future we want to be headed in. If you, or anyone else wants this tuff on your pc, that is your right, but I don't, and most other people don't either, especially considering the millions of pc's that this crap has been forced onto, read a few of the articles on this site an others to see what kind of distribution model they really have. 180Solutions won't be around for 70 years, wait and see. And I don't think you can compare tv commercials to adware.

   May 10th, 2006 at 3:39 pm

5. David Johnston says:

   For a good example of how to deliver TV over the internet, look at what ABC is doing here: http://dynamic.abc.go.com/streaming/landing

   They don't install any extra software on your PC (I think it uses Flash) and they can still deliver ads when you watch the show. There's no need to install any special ad-delivering software.

   May 10th, 2006 at 4:42 pm

6. Mark says:

   Can you say D'oh. Obviously the people at the WB are apparently lliving in their own world, or they are too lazy to do a little research beyond the obvious 'We are a great company' marketing BS from 180.

   May 10th, 2006 at 6:55 pm

7. MarcosV says:

   Interesting that bittorrent is tossed in the mix. So I get to pay $1 or more per TV episode or movie and have my precious uplink bandwidth taken up to boot?

   Can you use a standard BitTorrent client where you can see what's going on or something they force you to use with limited visibility on what's going on.

   I too wonder about what sort of games were being distributed by 180Solutions.

   May 10th, 2006 at 7:16 pm

8. Inglix the Mad says:

   JR

   Welcome to the 21st century - or maybe you are still in the 20th century - adware is what made network TV free for the last 70 or so years, and if you don't like the ads, then you turn off the TV and read a book.

   The difference is a TV advertisement won't crash my TV. Adware has an annoying tendency to be poorly written and crash computers. Oh and 180 games are similar to bejeweled and such from what I've seen. My friend's mom trashed the computer he gave her to use in two months with 180.Zango.Cash downloads.

May 10th, 2006 at 8:37 pm

9. Jasper says:

My guess is that WB just need to install some of the wonderful 180 tools on all their computers.

I'm sure one person out on the net knows how to use the ad ware to suck out some good films that we can get for free, after all that's what the 180 software do, installing back doors to your system.

May 10th, 2006 at 9:02 pm

10. Karl says:

As an alternative to listening to the howls of fear from the ill informed, you could try to watch one of the shows, understand the install and uninstall process and make an informed decision. I understand that it is easier to just moo with the cows but its likely better to understand the facts for yourself.

This is the future, JR is right. Free movies, tv shows, and games are what people want. If they did not, companies like 180 (and NBC, ABC, FOX, CNN, MTV, …) would all be out of business already unlike the movie studios which are trying really hard to find a way for people to continue to pay.

May 10th, 2006 at 10:45 pm

11. Inglix the Mad says:

Karl *This is the future, JR is right. Free movies, tv shows, and games are what people want. If they did not, companies like 180 (and NBC, ABC, FOX, CNN, MTV, …) would all be out of business already unlike the movie studios which are trying really hard to find a way for people to continue to pay.*

I'll tell you what. I'll introduce you to my little brother in college. He fixes computers. It usually takes two or three times at US$100-US$150 per repair (according to him), but I literally watched one parent drag every single one of their kids one visit. That parent then told them to listen (to my brother, the tech) and after he was done said "If this happens again, the computer will be disconnected from the Internet, the high speed will be canceled, and it will be formatted and reloaded with nobody's stuff being saved. Got it?"

Kids and older people who don't know crap about computers are the primary victims of adware. Kids will believe that things are really "free" (and they aren't) despite the warnings. Click-through EULA's don't help either. I don't believe that your standard TV requires installation either.

This bull is why standard TV will NOT go away. Karl, you and JR are just helping to perpetuate the culture of lies. 180Solutions software, in many cases, cannot be uninstalled without using a 3rd party utility!

Basically, if this is the future, get ready for your TV to crash.

May 11th, 2006 at 5:22 am

12. WTH says:

Wasn't 180solutions recently in the news for helping or distributing Kiddy porn?

May 11th, 2006 at 9:35 am

13. Dru says:

    Well I for one will be completely boycotting any company that works with any these idiots. So I won't be dealing with Warner Brothers, Sony, or Dell (MyWay Search Assist).

    May 11th, 2006 at 11:08 am

14. Bill M says:

    Thanks Dru — if anyone can get a complete list of companies using 180 I would like to have it so I can avoid them.

    May 11th, 2006 at 11:48 am

15. ReveNews - Jimmy Daniels says:

    More on WarnerBros and 180Solutions

    Okay, I'll admit I meant to follow up on my post about WarnerBros partnering with Zango, but it just completely slipped my mind until now, when I ran into a post on digg.com about it. And boy is it an…

    July 27th, 2006 at 6:18 am

16. Tech News and Tips from Tipsdr.com says:

    Kids, Cartoons and Adware

    Are screensavers really a problem? Asks a siteadvisor blog entry, and according to their results, they are, big time.
    We counted 318 children's television programs currently airing on English language networks in the United States. We decided to sear…

    September 4th, 2006 at 9:04 am

Leave a comment

Name (required)

Email (required)

Website

Submit

Ads by Google

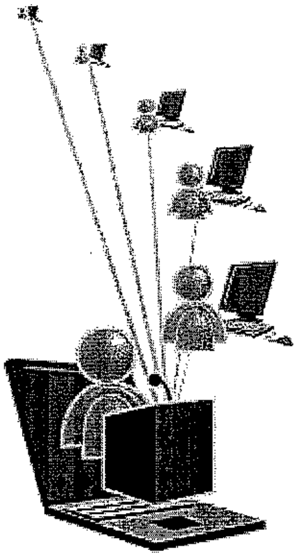
Which Spyware Remover?
Don't download any free Spyware remover until you read this article
www.CompareSpywareRe

Spyware Remover Download
Remove Spyware, Adware, Trojans & Keyboard Loggers. Rated 5 Stars!
www.pctools.com

Kill 180 Search Assistant
AntiSpywareBot Destroys 180 Search 5 Star Rated - Download 100% Free!
AntiSpywareBot.com

Spyware - Free Download
2006 Highly Rated Crash Resolver. Computer Freezing? Clean it!
NoAdWare.net

Paying Too
Much for
Online
Meetings?

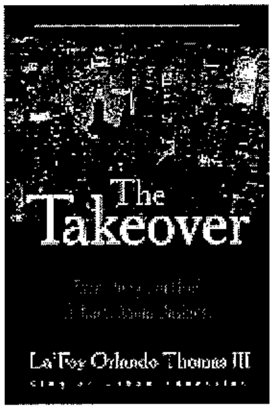


GoToMeeting™
ONLINE MEETINGS MADE EASY

TRY IT
FREE
CLICK HERE

BlogAds on
RealTechNews

Business & Investing
Guide For Wealth


The
Takeover
La'Foy Orlando Thomas III

The Takeover: Everything You Need To Know About Business, by LaFoy Thomas explains in understandable detail, Entrepreneurship, the stock market, bonds, real estate, mortgages, marketing, contracts, economics, legal business entities, accounting & more.

"Easy to Read & Understand"- BarnesandNoble.com

Read more...

Amazing Teas That Bloom Into Drinkable Bouquets

TEAS THAT BLOOM!
FREE SAMPLE

Full Bloom Tea has unique Teas that bloom into drinkable floral bouquets rich in antioxidants. Makes the perfect gift, or self indulgence for a Tea Lover. Free samples available. Check out our Demo of tea blooming on homepage.

Read more...

Business Broad

Some of us have secrets. The Business Broad doesn't.

Check out Business Broad for retail business secrets - budget tips, wholesale sources, and tricks of the trade.

No registration, no fees, no spam.

Read more...

Free cell phones in U.S

Sprint, T Mobile, Verizon Wireless, Cingular, Alltel, and more. Your choice of carriers, cell phones, and service plans. Online specials all the time. Free two day FedEx delivery. Get yours here.

Read more...

Advertise on RTN

PayPal DONATE

Please help us stay independent. Donate whatever you can today. (Even $1 will make a HUGE difference.)

About Us

RealTechNews is an award-winning independent blog about all things technical. We have over 40 dedicated contributors

Contact us | Tips

Free Newsletter

Your email address Subscribe

More Info

RSS Feed

Subscribe

Syndication

MY YAHOO!

Add to Google

XML RSS 2.0

SUB BLOGLINES

NEWSBURST

Awards

cnet NEWS.COM Blog 100

Feedster TOP 500 BLOG

THE SECOND ANNUAL
BLOG-X
AWARDS

©2006 RealTechNews | Underground Networks, Inc | Hosted by Dreamhost

Login:

Password:

Sign In

Lost Password?

Become a Member

Search:

All Articles

Search

Advanced Search

- Newswire
- Help
- Submit News

FANATICAL SUPPORT

rackspace MANAGED HOSTING

· Ads by Google Zone Labs Spyware Zone Alarm Freeware Zone AntiVirus ZoneAlarm Free Buy ZoneAlarm

Print this article | E-mail this article | Comment on this article

180solutions Drops Zone Labs Lawsuit

By Nate Mook, BetaNews

January 30, 2006, 3:47 PM

Adware provider 180solutions has voluntarily dropped a lawsuit it filed in November against security software vendor Zone Labs after claiming the company was making "false and misleading statements" about its products.

180solutions did not offer a reason for dismissing the suit; however, the company came under immense public fire after its actions were picked up by the press. Zone Labs' ZoneAlarm tool alerts users to the existence of 180's Zango software, and says it may log keystrokes and track Web sites visited.

180 claimed these accusations were false, alleging that ZoneAlarm caused "thousands of 180's customers to remove or otherwise uninstall Zango and/or 180SA," adding that, "180 has been damaged by the wrongful removal of its applications caused by ZoneLab's tortious conduct."

Although 180's Search Assistant and Zango tools may not be solely designed to spy on unsuspecting users, they do track what Web sites are being visited and deliver advertisements based on that data. 180 maintains that ads are delivered anonymously using a unique identification number.

But do users really want an application monitoring them in the background? Zone Labs and other anti-spyware vendors don't think

Ads by Google Advertise on this site

SAP for Midsize Companies
SAP Is For Great Companies, Not Just Great Big Companies. Learn Why
SAP.com/midsize

Kill 180 Search Assistant
SpywareBot Destroys 180 Search 5 Star Rated - Download 100% Free!
SpywareBot.com

so, and recommend removal of the software. Zone Labs said it did not make any changes to its software due to the lawsuit.

"From the inception of the suit, we believed it had no merit," said John Slavitt, general counsel for Zone Labs parent Check Point. "ZoneAlarm alerts are triggered by the behavior of a program, not its name. If the 180Solutions software exhibits suspicious behavior, we alert our customers accordingly. We did not make any concessions or reach a settlement after the suit was filed."

Shortly after filing its lawsuit against Zone Labs, 180solutions promised to clean up its act by ending the distribution of 180search Assistant and releasing Seekmo Search Assistant instead, which it said includes technologies to help reduce the number of unauthorized installations.

But some security experts, such as Sunbelt Software president Alex Eckelberry, remained skeptical. "Let's not forget that a crapload of 180 installs occur on sites that push an install on you that you don't actually need," he said in December.

Add a Comment (25 Comments)

BetaNews reserves the right to remove any comment at any time for any reason. Please keep your responses appropriate and ***on topic***. Foul language and personal attacks will not be tolerated.

Name (required):

E-mail (required):

Enter Your Comment:

Post Your Comment

By ***MarKomus*** *edited* Jan 31, 2006 - 10:08 AM

So now they will come out with a NEW product with BETTER safety features (Read: They will come out with the SAME product repackaged with EVEN MORE adware).

Score: **0**

Post a Reply

By ***athome*** *edited* Jan 31, 2006 - 8:20 AM

First 180 is doing nothing more when it logs the sites you visit and issues ads based upon that data. That is adware!

The real issue is that 180 corrupts registry data, steals resources, loads more crap onto your computer, and crashes the system. This is what people hate about the program. Zone Alarm is just giving you a heads up.

The whole issue of privacy is idiotic in the context that people use it. If you search on a search engine(GOOGLE, MSN, etc) they are keeping data on you - more than you know. Ironic that Google claims they are protecting your privacy, when they are abusing it to begin with. The entire Internet existence is built upon tracking you - from cookies to programs.

It has become such a mess with regard to adware defintions and antivirus software identifying and removing them. It isn't a matter of definition, but if "I" or "You" want them on our PC - for whatever reason we so choose.

Since we aren't given the option to install(most cases) such crapware, we should be given the oportunity to remove it. Not knowing all variations of the identification process, we in turn rely on those(Zone Alarm) whose business it is to identify. We installed those programs and tust the companies in their ability to identify and remove them. If this act is deemed illegal by ad companies, it will only be a matter of time before our computers will be loaded with them when we buy it from the shelf(which does happen already).

Our computer will not be ours, but belong to Dell, eMachine, HP, or Gateway and we will not be able to remove programs that they installed from the start. Have you ever looked at the new PCs of today and all the crapware that is loaded on. I tell all my customers that a PC is just a PC, but they should hire someone like myself to clean all the crap off their PCs when they first buy it, rather than pay a great sum of money to have the computer reinstalled after it has been corrupted by these companies.

Score: **0**

Post a Reply

By ***maniakmx3*** *posted* Jan 31, 2006 - 10:23 AM

Quote "Have you ever looked at the new PCs of today and all the crapware that is loaded on"

Lol, not only do we have Malware, Spyware, and Adware. We now have "Crapware". Oh well, has anyone seen my Crapware removal tool?

On a lighter note what athome state's is 100% correct. MSN is giving away our search data, (so all you porno weirdo's out there becareful) Google on the other hand does not, they do hold on to a partial amount of our data, but for search resouces. All google uses it for is to find out what people search most on the web so they can help server thier customers better. Google as of this moment is in the courts fighting for us and our privacy. Our government wants our data to use it to catch child pornography abusers, File Sharing etc. So pretty much don't use MSN if you curious and wanna see how a bomb is made, because you might have the FBI knocking on your door because THEIR curious on why you wanna know how to make a bomb.

As far as crapware goes, athome is right again. You buy a peice that wasn't custom, or atleast an alienware or an Acer, somthing along those lines. You're gonna have to call someone like us to come out to your home, or bring your computer to their shop, get charged so much an hour to get your PC cleaned up so it'll run the way it should. :)

Score: **0**

Post a Reply

By ***PC_Tool*** *posted* Jan 31, 2006 - 9:58 AM "they are keeping data on you - more than you know."

And your point? They can keep it all they want....that's private. It's when they start giving it away or selling it that it becomes a problem.

Score: **0**

Post a Reply

By ***athome*** *posted* Jan 31, 2006 - 11:26 AM

what do you think they are doing with it? I can't believe that you are this naive.

Score: **0**

Post a Reply

By ***PC_Tool*** *posted* Jan 31, 2006 - 11:34 AM

lmao..

Why do they *have* to be doing something with it?
I can't believe you are that paranoid.

Score: **0**

Post a Reply

By ***joeshmoe7*** *posted* Jan 31, 2006 - 12:22 PM

Maybe because they are 180 and they are EVIL dirtbags who would sell their own mothers souls to hijack your browser. Well thats just my opinion of them, their not the only ones out there but they are getting most of the attention lately. And on the surface, they try now to wear the cloak of legitimacy, but the sleeves dont quite cover up the tentacles.

Score: **0**

Post a Reply

By ***PC_Tool*** *posted* Jan 31, 2006 - 12:40 PM

Try reading the parent of the thread before adding to it.

Thanks.

(You might have noticed we were talking about search-engines, had you done so)

Score: **0**

Post a Reply

By ***joeshmoe7*** *edited* Jan 31, 2006 - 12:53 PM from parent - "The entire Internet existence is built upon tracking you - from cookies to programs."

Umm does that not include both (in reguards to keeping dats on us)? Oh well as you wish then.
It wasn't a shot at the search engines or cookies, just the programs. I took his argument to apply more to the adware since that is what the main article is about... perhaps that is my mistake then.

Score: **0**

Post a Reply

By ***PC_Tool*** *posted* Jan 31, 2006 - 2:25 PM

lmao..

Wow. Score 0 for reading comprehension.

My first reply to his included a quote from his post:

"If you search on a search engine(GOOGLE, MSN, etc) they are keeping data on you - more than you know."

This is what we were discussing. Capiche?

Score: **0**

Post a Reply

By ***joeshmoe7*** *edited* Jan 31, 2006 - 3:33 PM

i just said perhaps it was my mistake... Capiche? Score 0 for not reading my last line :)

Edit: yes i realize he brought up search engines, but he brought it up in the context of an article that has nothing to do with search engines, to what i thought was to make a point about collecting data, to which i was making the point that these adware companies collect data for nefarious purposes.. to which your comment seemed to me to point to...yatta yatta i have reading comprehension i don't however have mind reading. Oh forget it, chalk it up to miscommunication. It happens.

Score: **0**

Post a Reply

By ***PC_Tool*** *posted* Jan 31, 2006 - 3:35 PM

So it requires mind-reading to follow a thread?

We really don't need to get into this. All you needed to do was read the first post by me in this thread to have *not* replied looking like an ass.

You chose not to do that. No excuse needed, it happens to everyone. mmmmkay?

Score: **0**

Post a Reply

By ***joeshmoe7*** *edited* Jan 31, 2006 - 3:46 PM

I did read the first post by you, and in the context of the whole article and his comment, i felt you were replying in a more general way about the adware.. Again, it was my mistake. Actually yes sometimes i find it does require mind reading with some people :) (not necessarily you i mean people in general)

Score: **0**

Post a Reply

By ***PC_Tool*** *posted* Jan 31, 2006 - 5:51 PM

Heh...some people require... I concede your point.

Score: **0**

Post a Reply

By ***crashoverride*** *posted* Jan 31, 2006 - 1:15 AM

As well they should. Stupid dinks.

Score: **0**

Post a Reply

By ***wincement*** *edited* Jan 31, 2006 - 12:31 AM

I guess they realized they had a snowball's chance in hell at actually succeeding.

On a completely separate note, Alex Eckelberry is now cool in my book just because he said "crapload." =p

Score: **0**

Post a Reply

By ***joeshmoe7*** *posted* Jan 30, 2006 - 9:27 PM

Seekmo, another one i will be removing at every encounter. Die 180.

Score: **0**

Post a Reply

By ***Black-Wolf*** *posted* Jan 30, 2006 - 8:37 PM

Yeah........ just woke up

Score: **0**

Post a Reply

By ***zee7*** *posted* Jan 30, 2006 - 7:26 PM

Smart move. This may help stave off the inevitable bankruptcy a bit longer.

Score: **0**

Post a Reply

By ***eman8ions*** *posted* Jan 30, 2006 - 5:46 PM

"180solutions did not offer a reason for dismissing the suit"

How about the allegations not being either of "false and misleading...".

Score: **0**

Post a Reply

By ***lil2short2see*** *posted* Jan 30, 2006 - 4:39 PM

flashing ads on your computer after visiting a certain site makes me want to restore it, which i will not be very happy

Score: **0**

Post a Reply

By ***rijp*** *posted* Jan 30, 2006 - 4:33 PM

Can you say "OOPS!"

Score: **0**

Post a Reply

By ***GoodThings2Life*** *posted* Jan 30, 2006 - 4:16 PM

I'm sure someone on their "legal counsel" realized that their clients are idiots.

Score: **0**

Post a Reply

By ***bourgeoisdude*** *posted* Jan 30, 2006 - 3:58 PM

Maybe they thought...no, nevermind, I bet the main problem is that they DIDN'T think!

Score: **0**

Post a Reply

By ***maniakmx3*** *posted* Jan 30, 2006 - 3:49 PM

They dropped the suit because they realised it was stupid and unnessicary, just like their software. :P

Score: **0**

Post a Reply

Headlines

May 30 - 5:31 PM ET No Conspiracies Revealed by Novell 10-K Filing About Microsoft Pact

May 30 - 4:32 PM ET Certicom Patent Suit Against Sony Threatens to Unravel AACS

May 30 - 4:14 PM ET Tech Giants Push for NAND Flash Use in PCs

May 30 - 2:44 PM ET Palm Introduces New Laptop Product Line

May 30 - 2:36 PM ET CBS Acquires Last.fm for $280 Million

May 30 - 12:38 PM ET Where is Microsoft Going Today with Its Touch-Table 'Surface?'

May 30 - 12:35 PM ET DRM-free Music Arrives on iTunes

May 30 - 12:31 PM ET AT&T Debuts Smaller, Lighter BlackBerry

May 29 - 5:27 PM ET Broadcom Wins $19.64 M: Qualcomm Infringed on Three Patents, Says Jury

May 29 - 5:18 PM ET Update: Microsoft Hasn't Sold 1 Million Zunes

Windows XP & Internet Explorer 6 Selected

Instructions to increase PC & Internet speed.
Click "**Next**" now for a 2 minute PC tune up.

Next >>

<< Prev

© 1998-2007 BetaNews, Inc. All Rights Reserved.

The data
warehouse
project took _
FIND TECH JOBS
Dice™
The Career Hub for Tech Insiders™

Security MVP Porter discusses fences coming down. Jimmy Daniels talks ISP's & fed

Best of the Web Since 1994 60 Days Free Onlin
No Obligation. No Charges. No Kidding!

search blog Search Web ReveNews.com Browse By Author

Wayne Porter is one of the co-founders of **ReveNews.com**, and served as the CEO and founder of XBlock Systems before acquisition by IM security leader, Factime Communications. His projects include the popular **SpywareGuide** and the **X-RayPC Process Analyzer**.

His recent work includes working with the **Federal Trade Commission** to help shape spyware policy and his team's creation of two patent-pending technologies to contain unwanted software on corporate networks. Wayne is a frequent speaker at e-commerce business events. He received the Affiliate Summit 2005 Legend Award, named a Microsoft Security MVP and recognized by Google as a Security VIP for responsible security disclosure. Wayne currently works for **FaceTime Security Labs**, the one of the world's leading IM, Greynet and Web Filtering security companies, as the Senior Director of Special (Covert) Research.

His hobbies include reading science fiction, playing chess, fishing, writing, collecting shiny digital gadgets, playing raquetball and the study of memetic engineering. He maintains a personal blog at WaynePorter.com

[View All Entries By Wayne]

Random Links of the Moment

SecondLifeVideo.com
CostPerNews.com
JimKukral.com
BotSense.com
Blog.spywareguide.com
VitalSecurity.org

Links

Official Response from 180solutions to Porter's Questions

Filed under: Adware, Spyware & Greynets - April 02, 2005

Continued from Porter's Preface to 180solutions' Response.

While 180solutions was a bit late in getting their responses to me they did keep their word and have provided answers to my questions. In keeping with my promise to them I will keep the comments turned off and refrain from making m own comments on their responses in this blog entry.

Without further ado here are the questions and answers kindly provided to me b *Cory Magnus* of 180solutions. They are unedited and I have not verified or fact checked their claims. What you see is what you get. I will leave it to readers and analysts to make their own judgements and provide feedback in their own journals.

[ScreenShot Note: I have taken the liberty of compressing the screenshots in th original Word file because the image size would have made the entry download a unacceptable rate. However I have retained image dimensions as per the paper.]

[Reader's Note Questions are in Bold Format]

1.)Why was 180solutions admitted to COAST? What did kind of promises did 180solutions make in order to get into COAST?

> Part of COAST?s mission was to develop a program for software developers to join and contribute to setting standards around downloadable applications and online advertising. 180solutions strongly supports standards that will create a safer Internet, and wanted to gain membership in COAST to help create guidelines and best practices for software developers.
>
> 180solutions approached COAST in 2004 asking to work with the organization in an effort to improve our applications ? ultimately ending up with even better user notification, consent, and uninstall capabilities. 180solutions proactively made changes to both the application and distribution channel and as a result was welcomed to COAST in mid-January.

More information on our relationship with COAST can be read here:

http://www.180solutions.com/pages/pressrelease.aspx?node=/Press/COAST

2. Shortly after 180solutions was admitted to COAST, that organization collapsed when its three of its anti-spyware members (Webroot, Pest Patrol, Aluria) withdrew. Why then is 180solutions still touting its admission into COAST? (e.g. There is a prominent link on the 180solutions.com home page but also the report of Duane Jeffers at SpywareInfo: http://forums.spywareinfo.com/index.php?showtopic=26327.)

As is the case with many non-profit organizations, gaining consensus can at times prove challenging. Despite COAST?s organizational issues, 180solutions is steadfast in our commitment to operating under the highest set of standards for downloadable applications. 180solutions will continue to forge relationships with industry experts and advocates to improve the online experience and consumer safety. We recognize the need for best practices to be outlined, and will continue to work with other companies to put these standards in place.

Despite the organizational issues within COAST, 180solutions has embraced the recommendations made by the founding members of COAST and has implemented changes into the application and distribution channel. In fact, Sam Curry the vice president of product management for CA's eTrust brand told eWeek ?I find it odd that 180solutions is the source of the conflict. The goal [of COAST] was to certify vendors that reformed their product. 180solutions went to great pains to make major changes. The new versions of their software conform to scorecards and standards,? Curry said.

Curry further commented that ?he pinned the blame for the breakup squarely on the shoulders of Webroot and Aluria?.

3. 180 used to distribute software called nCase. I have been informed by members of your staff that you no longer distribute nCase. Why did 180 stop distributing nCase? What's the difference between the nCase software and the 180search Assistant and Zango programs that replaced it?

All applications evolve over time and become easier to use, more efficient and more feature rich. With each update applications offer more options and controls to users. It is the company?s No. 1 priority to provide value to users and develop a long-term, positive relationship with consumers. We will continue to enhance our applications and continue to survey our user-base for input on how we can improve.

180search Assistant represents the next generation of a line of products that included nCase and goes to back to the origins of the company. 180 started as a company which developed an advertising solution that was licensed to ISP?s who wanted to provide free internet access in exchange for an advertising window being displayed to the user whenever the user was connected to the Internet. That application and service evolved to where 180 was licensing its service to software developers under the nCase name.

Advertise on CostPerNews

Mention Code: ReveNews

HOT COMPANIES Info Security Products Guide 2006

FaceTime

BLOGSHARES premium MEMBER

Wayne Porter Date Archives

February 2007
January 2007
December 2006
November 2006
October 2006
September 2006
August 2006
July 2006
June 2006
May 2006
April 2006
March 2006
February 2006
January 2006
December 2005
November 2005
October 2005
September 2005
August 2005
July 2005
June 2005
May 2005
April 2005
March 2005
February 2005
January 2005
December 2004
November 2004
October 2004
September 2004
August 2004
July 2004
June 2004

Wayne Porter Recent Entries

Grazr- Widget to Graze Content for

Zay Does Affiliate Summit and Paging Shmuly

User Generated Ads- Brand Evangelists Participate and Create

Take Down The Fences- What or Who Will Show Up?

Todd Crawford- Affiliate Marketing Legend and Why...

Affiliate Summit West 2007 More Photos (77)

Seeking More Clarity on 2.0 Widgets and More

Web 2.0 Panel Pros, Cons, Clarity and Cash Registers...

Affiliate Summit West 2007 "Gonzo" Photos

Fear of Freezing in Las Vegas: Affiliate Summit West 2007 Part1

180search Assistant represents the next generation of nCase and features many enhancements including better performance; more user notification including labeling of the advertiser?s websites, a persistent system tray icon, as well as an easier uninstall process. Zango is an entirely new media model for sponsoring content online and is much more than a new piece of software.

4. What happened to all those older nCase installations? Did 180 upgrade them to the 180search Assistant? If 180 did that, did 180 notify those users first? If so how?

We upgraded the users at the same time we introduced the new, easier uninstall process.

5. There have been many reports of 180's software being stealth installed on people's computers. How did this situation happen? Are there still stealth installs going on? What is 180 doing to stop those stealth installs

First, 180solutions cares a tremendous amount about what users think about our software from how it is distributed to how it works on a user?s machine. As our company has grown, our company has and will continue to invest heavily in user-focused initiatives. Going forward, through the use of additional staff and innovative technology, we will dramatically increase control over how our partners operate. We understand and accept the responsibility to monitor and police our partners.

Historically, 180solutions has not installed software; we relied on a network of partners to distribute our applications. Over the last year, 180solutions has placed greater emphasis on managing distribution partners as well as moving to maintain more control over how our software is installed on users? machines. In response to public and our own concerns, we careful monitor our channels for conduct we find inappropriate. 180solutions has a stringent distributor code of conduct in place and frequently audits distribution partners. One of the reasons we were interested in working with COAST is that we hoped to develop an industry-wide distribution monitoring service as in part envisioned by Jay Cross, formerly of the The Internet Privacy Conservation Council (IPCC) and advisor to COAST.

If questionable practices are found, 180solutions investigates the situation and takes the appropriate corrective measures including legal action. As you can see we?re extremely clear in the 180 Distributor Code of Conduct:

Distributor agrees to accurately provide easy to read and understand notice and information to all end users of 180solutions products and all other applications that are bundled with 180solutions products before both initiating a download to and installing the products or applications on an end user?s computer, and to give such end user an easy and appropriate method to agree or not to agree to such installation. Distributor shall under no circumstances attempt to launch a 180solutions product executable without first displaying the above-described messaging and receiving explicit user consent for the installation. 180solutions reserves the right to approve final wording of this messaging and to require periodic changes as necessitated by changes to 180solutions products or for other business reasons. In addition, each installation of 180solutions products by

Distributor must include and be subject to the then current 180solutions End User License Agreement (EULA).

Distributor will ensure that the end user may easily remove/uninstall not just the 180solutions products, but each and every other application bundled with 180solutions products by using the Microsoft Windows Add/Remove Programs menu. Distributor will also ensure that all applications bundled with 180solutions products adhere to terms no less restrictive than those contained in this Agreement follow these same codes of conduct. Other products or applications that act as program ?Trojans? (installing additional applications without full product descriptions and EULA acceptance) shall not be bundled with any 180solutions product.

When we find credible and verifiable examples of installs that violate our Code of Conduct and undisclosed installs certainly would, then we take immediate action including but not limited to terminating the partner and suing them as we did last summer.

5. How does 180 distribute its software? Your web site says that you use 'distribution partners". Were some of these partners responsible for the stealth installations of 180's software? What is 180 doing to make sure that this sort of problem doesn't crop up again with its partners?

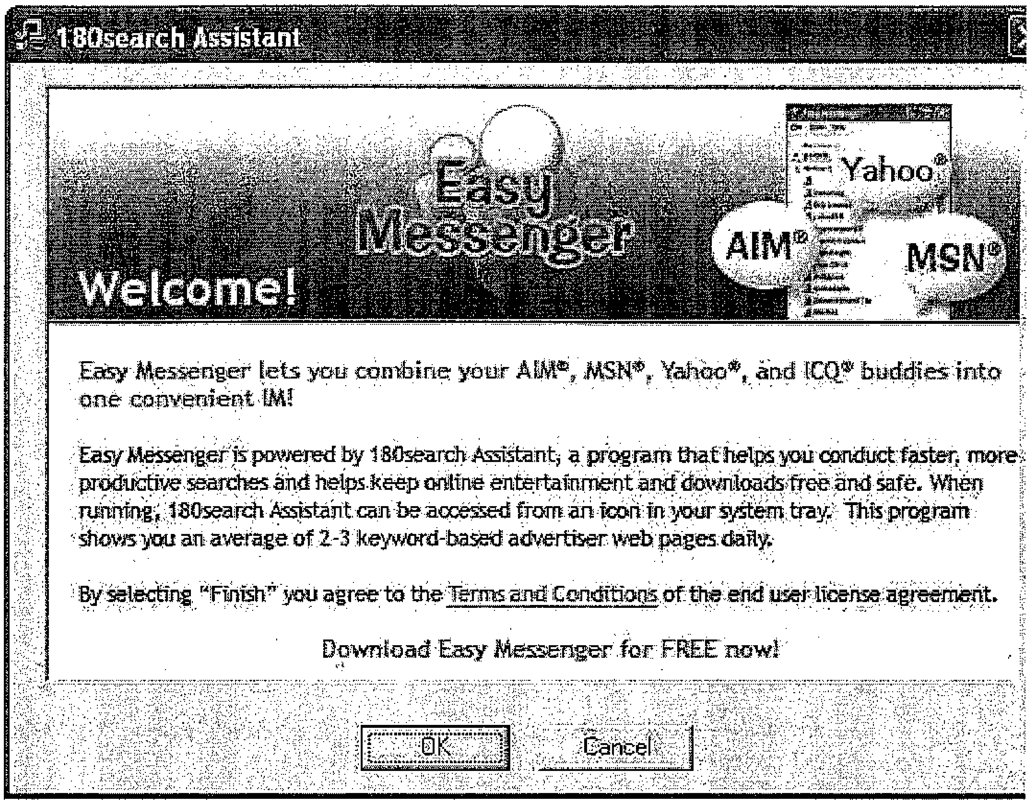
180solutions software is distributed on our websites and through distribution partners who promote their software and web services with support from 180.

180solutions distribution partners only install our applications once user notification and consent have taken place. 180solutions carefully screens potential distributors and rejects 9 out of every 10 who approach us. We monitor the activity of all distribution partners. Any strange or inappropriate activity is immediately investigated. Distributors found in violation of the company?s distributor code of conduct are subject to legal action. When provided with credible evidence, we will and have sued former distributors.

We are also taking steps by introducing new technology into our applications. The newest versions of our software have two important changes that we expect will provide not only ourselves protection but our users from bad actors. In addition the newest versions of our applications have been fundamentally changed in what gets distributed and how our application is installed on a user?s machine. First, we only distribute an installation file whose purpose is to verify a user?s intent to install. Then once that consent has been confirmed through a prompt like the one below, the installer file will call to our servers and download the application. This will solve any going forward issues of old code circulating in various distribution channels as well as allow us to more tightly control our distributors.

Example Prompt:

Copyright © 1998-2006, ReveNews, LLC. All rights reserved. Privacy policy. D.M.C.A Notice. Advice Archives Design by


180search Assistant
Easy Messenger
Welcome!
Yahoo®
AIM®
MSN®
Easy Messenger lets you combine your AIM®, MSN®, Yahoo®, and ICQ® buddies into one convenient IM!
Easy Messenger is powered by 180search Assistant, a program that helps you conduct faster, more productive searches and helps keep online entertainment and downloads free and safe. When running, 180search Assistant can be accessed from an icon in your system tray. This program shows you an average of 2-3 keyword-based advertiser web pages daily.
By selecting "Finish" you agree to the Terms and Conditions of the end user license agreement.
Download Easy Messenger for FREE now!
OK
Cancel

7. 180 has millions of installations of older versions of 180search Assistant. Many of those may have came from stealth installs where users didn't know the software was being installed. What is 180 doing about those existing installations of older software? Will 180 remove them or keep them?

The notion that many of our users came from improper installs is an urban legend started in the anti-spyware community. Unfortunately there is a fair amount of public hysteria in the press these days about malicious software. The reality is that 80% of so-called spyware are harmless cookies.

As we have discussed, in cases where we find credible and verifiable evidence of wrongdoing we take many steps including terminating and even suing those distributors accused of wrongdoing. In those cases we notified users by showing this message:

We are currently upgrading all versions of our application to reflect the changes recommended by COAST. If, after the upgrades are made, we find new installs of our older product being distributed we will turn off those applications and pursue the distributor for violation of the Code of Conduct.

180solutions provides toll-free customer support so users can contact us directly with questions and concerns about our software, installation and uninstall methods. 180solutions doesn?t intend to be installed on a computer where we are unwanted, and encourage any user who feels they received our software by mistake to follow uninstall instructions.

180search Assistant

Dear 180search Assistant customer,

You have received this message to ensure that you are aware that 180search Assistant is installed on your computer.

180Search Assistant was likely installed when you downloaded the ABC Search toolbar or i-lookup toolbar.

- 180search Assistant is an application that delivers you on average 2-3 targeted websites daily to enhance your search and shopping activities online and also supports our partners so they can provide you with content and downloadable software, such as toolbars and screensavers, for free.
- The targeted websites are identified with "Brought to you by 180search Assistant" at the top of your browser window.
- 180search Assistant does not collect any personally identifiable information.
- 180search Assistant collects anonymous information about the websites a user visits in order to show targeted comparison websites.

You can choose to uninstall the 180search Assistant at any time by going to "Add/Remove Programs" in your control panel and selecting 180search Assistant. For more information, see our FAQ.

8. There are reports the new 180search Assistant has a prompt screen that displays when the software installs for the first time. But what happens when an older version of the 180search Assistant calls the 180 servers to check for updates? Will those older versions be allowed to update to the new versions? If they are allowed to update, will the new prompt screen display?

------------------------------ See Response to Question 7 ------------------------------------

9. Could you describe the advertising that 180 displays on people's computers? How is that advertising labeled?

All advertisements displayed by 180solutions software are opened in a second browser window and presented as a Web site, rather than an advertisement. The second browser window opens, and functions exactly the same as any other page opened in a browser. The window is clearly labeled in the title bar as either or ?Brought to you by the 180search Assistant,? depending on the software installed on that machine. The page may be closed simply by clicking on the ?X? in the top right corner of the page.

180solutions advertisements are all triggered real-time by keywords in the URL line. For example, if a user is searching on various search engines for Alaska cruises, a Web site for one of our advertisers selling Alaska cruises may appear in a second browser window, offering a listing of prices to purchase an Alaska cruise. This offers the user additional information to what they are browsing for online. There is no profiling and no capture of any browsing history.

10. 180 is getting a lot of flak right now, and perhaps this flak is well deserved giving the issue of stealth installs. Why do you feel anyone should trust 180 Solutions after all the things that happened before?

If you were to visit 180?s offices you would see a bright, vibrant community of talented people who would compare well to any other well known Seattle-based companies.

180solutions enriches our trustworthy relationships with over 20 million consume by giving away more than $1 million of premium content each month. 180solutic serves more than 5,000 advertisers, providing them with targeted traffic to their Web sites. The company has made serious efforts to create the best and safest user experience possible and protect its users? privacy. 180solutions partners wi more than 50 content providers and has acquired an instant messaging development company and local game development studio. We will continue to pursue relationships with premium content providers to offer our users the best online entertainment. In less than one year, we have become the 15th most trafficked gaming Web site.

Washington-based 180solutions is recognized as one of the fastest growing priva companies in Washington and in the U.S., a best company to work for in Washington, and a high-tech leader in Washington by respected publications including the Puget Sound Business Journal, Washington CEO and Inc. Magazine Organizations including the WSA (www.wsa.org), Venture All Stars (www.ventureallstars.com), and The Pacific Northwest Friends of FSH (www.fshfriends.com) have noted the company as a successful business leader i the community. 180solutions provides real person customer support to its users and is actively involved in bettering the Internet.

11. Are you getting taken out of anti-spyware programs so that they dor detect your programs any more? If so, which ones?

We are in conversations with every company in this space that we can find ? and we are definitely not alone in that regard. These companies have used very aggressive criteria and lists that now encompass so many types of software and technologies we feel do not justify the inclusion of our software. So far a handful has removed the latest versions of our applications.

12. What else do you think people ought to know about 180solutions an the changes it's making to its software?

180solutions is structured and operates like any other media company. Just like NBC we are in the business of connecting advertisers to consumers, and providing entertaining, free content. One wouldn?t look at NBC and call the network ?advervision? ? but clearly NBC is in the business of showing advertisements that sponsor content. 180 does the same thing.

Each day we ask ourselves ?what could we be doing better?? ?how can we make it even easier for consumers to find what their looking for?? ?what content do consumers want and how can we sponsor that?? ?how can we improve our application today??. We?re proud of our accomplishments and will continue to innovate and help shape an ideal online experience.

Our company is all about adding value to consumers, advertisers, and Web publishers. We recognize the importance of providing a positive experience for each one of these groups and continually work to enhance our application. It?s important to note that 180solutions exceeds all standards either proposed in pending legislation or in enacted laws for downloadable applications/Internet advertising. The company was the first keyword search advertising provider to put an icon on the users desktop and system tray, clearly label each add, list our application in system processes, and make it simple for users to uninstall. Unlike other players in the space, we only show on average 2-3 ads per active user per day and the vast majority of users see no ads on a given day. By showing fewer ads and making those highly relevant to what consumers are looking for we are able to create a better service for our users.

--End of Interview--

Porter's End Note: I strongly encourage bloggers, consumers and industry analys or other software makers to formulate their own responses and opinions and trac back to this entry so we can keep a civil dialogue going and get more answers to mportant questions. There will be no forward movement on issues until we start communicate and most importantly understand each other?s unique position.

Ping's Can Be Sent Here: http://alpha.revenews.com/MT/mt-tb.cgi/515

Permalink   Email this   Add to del.icio.us

Trackback Pings

TrackBack URL for this entry:
http://www.revenews.com/MT/mt-tb.cgi/515

Listed below are links to weblogs that reference Official Response from 180solutions to Porter's Questions:

» Wayne Porter on 180 from Sunbelt Blog
To those of you following the whole "is 180 Solutions making products that deser the adware/spwyare moniker?" debate, Wayne Porter just posted some interestir stuff on his blog. Mr. Porter, who runs a company that makes a competitor to oui Counter... [Read More]

Tracked on April 2, 2005 11:02 PM

» 180solutions Responds to Wayne Porter, but Did They Answer Him? from Affilia Program Tip Blog
Back in March, Wayne Porter challenged 180solutions to answer a series of questions on their business practices and such. In Wayne's blog, Cory Magnus of 180solutions protests that "The notion that many of our users came from improp nstalls is... [Read More]

Tracked on April 3, 2005 06:51 PM

» Scratch a Lie, Find a Thief from Spyware Warrior
A few days ago I published an interview with Jay Cross, former researcher for the Consortium of Anti-Spyware Technology Vendors, which got into hot water with t anti-spyware community and eventually collapsed after is granted membership tc 180solutio... [Read More]

Tracked on April 4, 2005 12:17 AM

» Beware of Metrics Direct (A.K.A. 1800solutions) from Internet Marketing .co.in
Metrics Direct (1800 Soultions) answers to questions by Wayne Porter. MetricsDirect uses software (spyware) to get on computers through automated downloads. Computers with Windows XP SP2 (Service patch 2) update may be stopping most of this. Another... [Read More]

Tracked on April 4, 2005 10:07 AM

» Merchants, Investors and thoughts on 180solutions from ReveNews: Beth Kirs
Wayne Porter has an opened an interesting discourse with 180solutions recently. had been picked up by Spyware Warrior, Shawn Collins, and others. Stewardshi of the internet is the heart of the matter over Zango, n-Case and other 180solutions' appli... [Read More]

Tracked on April 5, 2005 02:42 PM

» 180solutions Tops the List from Spyware Warrior
That is, the list of most detected malware, according to Emisoft, the company th makes a-squared malwre remover. This list reflects their findings in just the last days (note the page has today's date on it), on the Spyware, Adware, Ad supported ... [Read More]

Tracked on April 6, 2005 05:48 PM

» Oh, what a tangled web we weave... from Spyware Warrior
On Friday CNET reporter John Borland revealed that 180solutions had bought CD Inc. of Mont-Royal, Quebec. 180solutions, you'll recall, has been claiming for so time that it has cleaned up its act. It's even been crowing about its admission in th... [Read More]

Tracked on April 10, 2005 03:40 AM

» Spyware Installation Methods from Spyware Warrior
Ben Edelman's new article is so very pertinent right now. We just saw installatio without EULAs of adware and spyware in my write up on installs of 180solutions and other adware/spyware. So-called "adware" companies say nonconsensual installa... [Read More]

Tracked on April 12, 2005 12:22 AM

» !80 Solutions Re-Revisited Metallica Style- The YapBrowser from ReveNews - Wayne Porter: Greynets, Malware, Adware & Spyware Research- E-commerce
While Direct Revenue wrestle with their own problems explaining to Mr. Spitzer and nail.exe it appears 180 Solutions has some explaining to do as we see yet another nail driven into the proverbial coffin. Much less a nail but more like someone took a s... [Read More]

Tracked on April 17, 2006 02:30 PM

» Yapbrowser...Not Something You'd Want to Plugin To! from The Greynets Blog
This one has crept across the security pros and analysis can now be found here and here. For those not in the know, Yapbrowser is a browser "search tool" - unfortunately, none of the paid for links work (returning a... [Read More]

Tracked on May 6, 2006 03:11 AM

Email This Entry

Email this entry to:

Your email address:

Message (optional):

Send

ReveNews Sitemap

ADVERTISING
Save up to 75% on Cruises!
Last-minute deals from top cruise lines. GO

BUSINESS

MONEY & MARKETS
Get Quote
Stocks
Local stocks · Quickrank · A-Z List · 52 Week High/low · Index Performance · Market Movers
Mutual Funds
Quickrank · A-Z List
ADVERTISING

Tuesday, June 28, 2005

You may have this adware hidden on your computer

By JOHN COOK
SEATTLE POST-INTELLIGENCER REPORTER

180solutions has begun notifying 20 million people that the company's ad-serving software may have been installed on their computers without their consent.

The notifications, which started yesterday in the form of a pop-up message, is part of an effort by the Bellevue adware company to clean up its network amid intense criticism of past installation tactics.

"We want to make sure that every customer we have knows we have them," said 180solutions spokesman Sean Sundwall. "At the end of the day, it does us no good to have customers that don't know that our software is on their machines."

Sundwall estimated that less than 5 percent of the company's installations have occurred through distributors who did not properly inform customers. About 85 percent of the company's user base is receiving online advertisements through an older product called 180 Search Assistant, with the remainder using a product called Zango.

In a statement, 180solutions Chief Executive Keith Smith said, "Protecting consumers from bad actors and nefarious distributors is of the utmost importance to 180solutions."

180solutions, whose software delivers pop-up advertisements to people based on the Web sites they visit, has been accused by anti-spyware advocates of covertly distributing its software to millions of users. The company's admission to the Consortium of Anti-Spyware Vendors in January led -- in part -- to the disintegration of the organization.

While it is well-documented that 180solutions' software has been placed on computers without the user's consent, the company said it is taking steps to solve the problem. So far this year, Sundwall said, the company has eliminated 442 "rogue distributors" of the 180solutions software. In April, the company bought its largest distributor in effort to get better control of its network.

The notification being sent does not provide an uninstall button, although it does tell people how to remove the program. It also provides links to the company's privacy policy, end user license agreement and uninstall instructions.

The message does not provide a phone number or e-mail for customer support, although Sundwall said it is an easy five-step process. He added that the company will notify users more than once.

"Frankly, we need to continue to scrub our customer lists and only have people who want to be there," he said. "That is how we prove value to our advertisers and prove value to our customers."

One of the fastest-growing software companies in the state, 180solutions posted revenue of about $50 million last year. It raised $40 million in financing last year -- one of the largest venture capital rounds in the state.

Sending out notifications is a risky move because the company relies on having a large base of users in order to justify relationships with advertisers. But it is one that critics of the company have recommended in the past, with some others suggesting that the company simply turn off its old network and start over.

Sundwall said that he did not know if the notifications would cut into the privately held company's financial performance. But he said the company anticipates "very little, if any, downtick in sales."

Sundwall said that Esther Dyson, a well-known technology guru, suggested recently that the company notify users about the software.

"I would probably give Esther some credit for hatching the idea," Sundwall said.

"But she never really applied pressure, it was really more in passing to try this and see if it would work."

Buy Any Color
Chocolate™
For $99.99
Get the original FREE
WITH NEW 2 YEAR ACTIVATION PER PHONE AFTER $50 INSTANT ONLINE REBATE.
• Messaging Capable
• MP3 Player
• V CAST Music & Video Capable
View Plan Offer
LG CHOCOLATE
Get A Taste
verizonwireless

PAST COVERAGE

- Online marketer faces 'thiefware' accusations
- Internet advertiser disputes 'adware' label
- Anti-spyware group unravels over direction
- 180solutions lands a $40 million deal

P-I reporter John Cook can be reached at 206-448-8075 or johncook@seattlepi.com

E-mail this
Print this
E-mail newsletters
RSS

Save and share this article
del.icio.us Digg Facebook Newsvine

Add P-I Business headlines to
My web site My Yahoo! Google More options

BUSINESS HEADLINES
· Google has fun with hiring -- but tug of war talent is no game
· Some purchases give charities a boost
· Midsized banks on way back
· Saving planet can pay the bills
· Oil prices fall as strike in Nigeria ends
· In Silicon Valley, lunch is food for thought
· Manufacturing a big part of state's economi recovery
· Northwest Airlines' bumpy ride out of bankruptcy
· Philippine Airlines doubles its order for Boei 777s
· 300 million bottles later, Two Buck Chuck turns 5
· Barbara Cox Anthony dies; KIRO/7 part of h empire
· Business Briefing
more

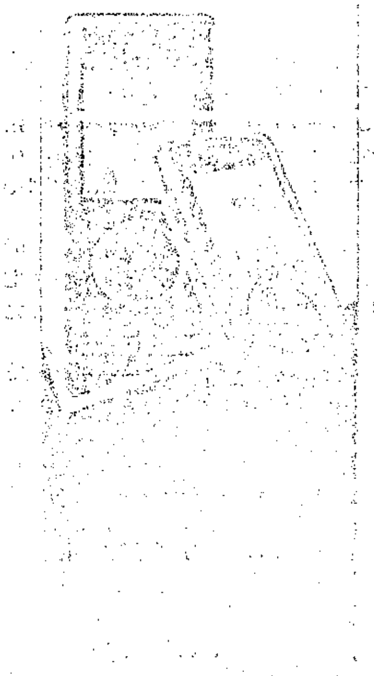
ADVERTISING

Treo 755p Official Site
Palm Smartphone w/ Broadband Speeds As Low As $279. Free Overnight S&H
Palm.com

Refinance - Save $1,000's
$150,000 Mortgage for $483/month. Four free quotes. No Obligations!
www.pickAmortgage.com

Loan Rates Near 39-Yr Low
$430,000 for $1299/Mo. Think you pay too much? Calculate new payment.
Mortgage-Rates.lowermybills.com

Buy a link here



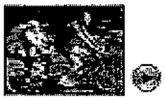
AP BUSINESS HEADLINES
- VeriSign CEO Sclavos suddenly resigns
- World Bank Bush Summary Box
- Stocks up slightly ahead of Fed minutes
- Tishman, Lehman to buy Archstone-Smith
- Oil prices lose more than $2 a barrel

›› more

AP HIGH-TECH HEADLINES
- IBM's buyback binge includes $11.5B loan
- Google-DoubleClick deal draws attention
- Moroccans cut off from YouTube
- Fitness vibrations trendy, perhaps risky
- GoDaddy agrees to run domains in limbo

›› more

VIDEO


Good Question: Which IRA Should I Choose?

On the Money: Tips on Shopping for Charity

Government Analyst Testifies on High Gas Pric

›› more videos

SEATTLE BLOGS

Todd Bishop's Microsoft Blog
- Microsoft's Novell deal: The word puzzle
- Microsoft angles for vacant Ninten land
- Pink is No. 2 Zune

John Cook's Venture Blog
- InfoSpace reportedly discussing $1 billion buyout
- Seattle recruit heads off to Y Combinator
- Eighteen-year-old introduces Scriptovia

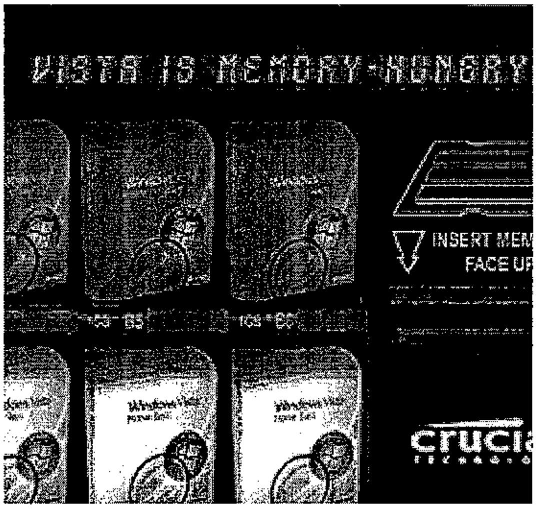
James Wallace on Aerospace
- Is Airbus about to make a major A350 design change? Also, more on those 787 fasteners
- 787 wings-- to break or not to bre that is the question
- Fasteners ... and the 787

ADVERTISING

Home | **Contact Us** | **About the P-I** | **Front Page** | **Corrections** | **P-I Jobs** | **Home Delivery** | **E-edition** | **RSS** | **Mobile Feeds** | **P-I**

Seattle Post-Intelligencer
101 Elliott Ave. W.
Seattle, WA 98119
(206) 448-8000

Home Delivery: (206) 464-2121 or (800) 542-0820
seattlepi.com serves about 1.7 million unique visitors
and 30 million page views each month.



more videos

Send comments to **newmedia@seattlepi.com**
Send investigative tips to **iteam@seattlepi.com**
©1996-2007 Seattle Post-Intelligencer
Terms of Use/Privacy Policy

The Effect of 180solutions on Affiliate Commissions and Merchants

Benjamin Edelman - Spyware Research, Legislation, and Suits

[Overview - Background - Methodology - 180's Actions & Effects - Discussion - Response - Disclosures]

Software from 180solutions (also known as MetricsDirect) redirects many affiliate commissions to 180. As a result, merchants pay commissions to 180 (and its advertiser partners) even when no commissions are payable under the terms and conditions of merchants' affiliate programs, and even when commissions are properly payable to other affiliates. 180 causes these commissions to be paid via at least 84 different affiliate accounts, using multiple intermediary domain names that redirect affiliate tracking HTTP traffic, making 180's activities particularly difficult to track and to prevent.

Related Projects

WhenU Violates Own Privacy Policy *(NEW)*
WhenU Advertisers *(NEW)*
WhenU Spams Google, Breaks Google "No Cloaking" Rules
Documentation of Gator Advertisements and Targeting
"Spyware": Research, Testing, Legislation, Suits
Other Research by Ben Edelman

Overview & Summary

Some web sites ("merchants") pay commissions to independent third-party web publishers ("affiliates") who recommend and link to merchants' products. Proper tabulation of affiliate commissions relies on a multi-step process, requiring coordination by merchants, affiliates, and (often) affiliate networks who help track the transactions. (Details about affiliate programs.) Software from 180solutions (also known as MetricsDirect) interferes with this tracking process, seizing affiliate commissions for 180's benefit and for 180's advertiser partners.

In my testing, 180 software specifically and systematically causes merchants' tracking systems to conclude that users reached merchants' sites thanks to 180's efforts, even when users actually reached merchants on their own or through other affiliates. As a result, merchants pay commissions to 180 even when no commission is properly payable (under affiliate program rules); i.e. when users reach merchants' sites without receiving bona fide recommendations from independent affiliate web sites. In addition, 180 causes merchants to pay commissions to 180 even when commission is properly payable to other affiliates -- who actually recommended, encouraged, and facilitated users' purchases from the merchants.

To seize affiliate commissions, software from 180 must first become installed on users' PCs. See discussion in 180solutions Installation Methods and License Agreement.

Once installed on users' PCs, 180 software performs four main functions:

1. 180 transmits to its servers information about the web sites that users visit. Each transmission bears a domain name (or other trigger condition), as well as a unique user ID that lets 180 build profiles of users' online activities. (details)
2. 180 shows popup ads, which generally cover substantially all of the targeted web sites. In my testing, 180 typically covers web sites with the sites of their competitors. (details)
3. 180 shows duplicate copies of merchants' sites, where the second copy has been reached via an affiliate link. As a result, merchants pay commissions to 180 (and its advertisers) on the resulting purchases. (details)
4. 180 opens hidden windows with invisible copies of merchants' sites, where the invisible sites are reached via affiliate links. As a result, merchants pay commissions to 180 (and its advertisers) on the purchases of affected users. Since 180's activities are silent and (to a user watching the computer's screen) invisible, this behavior is particularly difficult to detect. (details)

180's activities have attracted attention from some targeted merchants, leading some merchants to remove 180 from their affiliate programs (details). (Nonetheless, at least 300 major online merchants remain affected. (details)) 180's activities have also attracted attention from affiliates who are upset to lose commissions when 180 overwrites their tracking codes. (details)

To date the two largest affiliate networks (LinkShare and Commission Junction) have failed to remove from their networks all affiliates using 180solutions, despite behavior that seems to violate the networks' rules. (details) In the short run, the affiliate networks benefit financially from 180's activities -- even as merchants, other affiliates, and users suffer. (details) Meanwhile, the next-largest affiliate network (Shareasale) has removed 180 from its network. (details)

Background

Return to top

Computer users have recently come to face a growing array of programs that get installed on their computers (often without their knowledge, consent, and/or informed consent), and perform functions users dislike (often including tracking or transmitting personal information, or displaying targeted advertisements). Some programs redirect requests for particular web sites to other web sites; some cover advertisements with other advertisements; still others, including programs from Claria and WhenU, monitor and transmit sensitive user information and show targeted advertisements.

Programs from 180solutions monitor users' activities and show targeted advertisements, but 180 programs also overwrite affiliate commissions to cause 180 to receive payments from merchants when users make online purchases. Such behavior is not unknown. In September 2002, the New York Times published "New Software Quietly Diverts Sales Commissions," using the term "*stealware*" to describe software that "*divert[s] sales commissions*" by causing "*all future purchases [to] look as if they were made through the software maker's site, even if they were not.*"

Indeed, my research is not the first to report such practices by 180solutions. In November 2003, MSNBC reported that during September 2003, 180 had earned more than $100,000 in commissions from more than $4 million of purchases at Dell through this practice. Since December 2003, forum participants at ABestWeb (and elsewhere) have documented large-scale affiliate code overwriting by 180solutions software. (1, 2, 3, 4, 5, 6, 7, 8, 9, 10).

Notwithstanding this prior research as to stealware generally and even as to 180solutions specifically, I intend my research to make the following contributions: 1) To be more comprehensive in the scope of testing, checking 180 targeting of more than 166,000 trigger conditions. 2) To clearly report major online merchants targeted by 180, and to report major affiliate networks that facilitate 180's activities. 3) To be particularly rigorous in methodology, documentation, and proof, and to propose a methodology for further testing and reporting. In the sections that follow, I present a methodology for rigorously examining the activities of 180's Zango software, and I show the results of my examination, including a list of affected merchants.

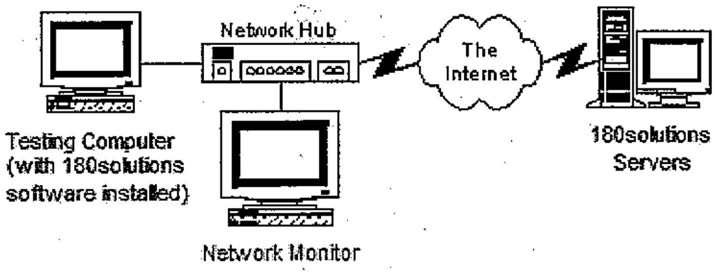
My research should be of particular interest to those advertisers and merchants who, intentionally or not, contributed to 180's $19 million of 2003 revenue, as well as the investors at Spectrum Equity who recently provided 180 with $40 million of financing. My research may also be of special interest to the 20 million users who reportedly currently run 180 software.

Before examining 180's effects, it is first important to understand how 180 software gets installed on users' PCs. For details, see 180solutions Installation Methods and License Agreement, which details installations through drive-by downloads, distribution partners, and security holes, as well as installations without license agreements or with only minimally visible license agreements.

Methodology & Transmission Format

Return to top

Consistent with the methodology explained in my prior articles about advertisement-display software (e.g. Documentation of Gator Advertisements and Targeting, WhenU Violates Own Privacy Policy), I installed 180solutions Zango software on a dedicated computer in my lab. Using a network monitor, I watched 180 Zango's transmissions over my own Internet connection. The design of my network is shown in the diagram at right. Capable as network monitoring may be, note that it's not properly called "snooping" or "wiretapping" (despite occasional allegations to the contrary): I can only monitor the transmissions made to and from my own computers.



Although I have tested software from 180 for roughly the past year, this article describes only behaviors that I observed in June-July 2004.

On my computer with Zango installed, I observed a file cryptically named kyf.dat. Opening this file in an ordinary text editor, I found that it listed 166,246 words and phrases, including the domain names of most major web merchants with affiliate programs, as well as other major e-commerce sites. Comparing these words to 180's subsequent behavior, I observed that when a user browses to a web page that includes these words (in the page's URL and/or in some portion of its page text), 180's software sends a message to the `tv.180solutions.com` web server, of the form shown below. Note inclusion of a trigger condition (yellow) and unique user ID (green). This transmission is reported below precisely as viewed by my network monitor, except that I have replaced my unique user ID with another similar value.

```
GET /showme.aspx?keyword=delta.com&did=762&ver=5.9
&duid=531byhiprtvdgvadrfmfcgtxxyrjmg&partner_id=195252523
```

keyword trigge

```
&product_id=762&browser_ok=y&rnd=21&basename=zango
&tzbias=5&MT=8C5F0B5F1538C31DC2F456CC736BC33B268398A0
&DMT=8C5F0B5F1538C31DC2F456CC736BC33B268398A0&bid=0&SID=ANCVAXYV
&OS=5.1.2600.2&SLID=1033&ULID=1033&TLOC=1033&ACP=1252&OCP=437
&DB=iexplore.exe&IEV=6.0.2800.1&TPM=200785920&APM=41066496
&TVM=2147352576&AVM=2006102016&FDS=1834094592&LAD=1601:1:1:0:0:0&WE=5
```

user i(

180's `tv.180solutions.com` web server then responds with instructions of the following form, often referencing an ad to be shown (pink) in a window with particular characteristics (orange). 180's Zango software, on users' PCs, reads and follows these instructions.

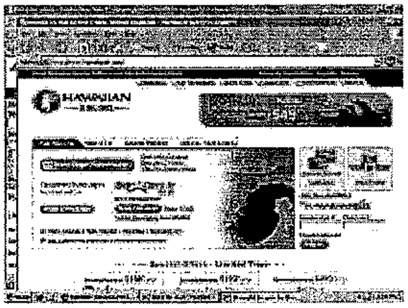
```
HTTP/1.1 200 OK
  ...

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<HEAD>
<meta name="vs_targetSchema" content="http://schemas.microsoft.com/intellisense/ie5">
</HEAD>
<body>
ncase_ad_url: <input id=ncase_ad_url name=ncase_ad_url
value=http://view.atdmt.com/AVE/view/www18haw002deltaXcom0001ave/direct;wi.800;hi.600/01/><br>
ncase_ad_width: <input id=ncase_ad_width name=ncase_ad_width value=800><br>
ncase_ad_height: <input id=ncase_ad_height name=ncase_ad_height value=ad_height
value=600><br>
ncase_ad_takefocus: <input id=ncase_ad_takefocus name=ncase_ad_takefocus value=y><br>
ncase_ad_activationdelay: <input id=ncase_ad_activationdelay name=ncase_ad_activationdelay
value=0><br>
ncase_ad_resizable: <input id=ncase_ad_resizable name=ncase_ad_resizable value=y><br>
ncase_ad_scrollbars: <input id=ncase_ad_scrollbars name=ncase_ad_scrollbars value=y><br>
ncase_ad_menubar: <input id=ncase_ad_menubar name=ncase_ad_menubar value=y><br>
ncase_ad_statusbar: <input id=ncase_ad_statusbar name=ncase_ad_statusbar value=y><br>
ncase_ad_toolbar: <input id=ncase_ad_toolbar name=ncase_ad_toolbar value=y><br>
ncase_ad_addressbar: <input id=ncase_ad_addressbar name=ncase_ad_addressbar value=y><br>
ncase_ad_fullscreen: <input id=ncase_ad_fullscreen name=ncase_ad_fullscreen value=n><br>
ncase_ad_statustext: <input id=ncase_ad_statustext name=ncase_ad_statustext value=><br>
ncase_ad_theatermode: <input id=ncase_ad_theatermode name=ncase_ad_theatermode value=n><br>
ncase_ad_id: <input id=ncase_ad_id name=ncase_ad_id value=335681><BR>
ncase_keyword_id: <input id=ncase_keyword_id name=ncase_keyword_id value=160802><BR>
ncase_ad_windowtitle: <input id=ncase_ad_windowtitle name=ncase_ad_windowtitle value="Brought to
you by the Zango Search Assistant"><br>
...
<INPUT ID=ad_shown TYPE=text VALUE="y" style="VISIBILITY: hidden;"><br>

<SPAN class="957085619-06032003"><FONT face="Arial" color="#ff0000" size="5">Thank you
for your patience.&nbsp; You will be redirected to your destination site in a
few seconds.</FONT></SPAN>
</body>
</HTML>
```

ad to be showi

ad characteristic:



Notice that the instructions above reference an ad ("www18haw002...") to be shown when I browsed to `delta.com`. Indeed, these instructions caused 180's Zango software to show an ad for Hawaiian Airlines that covered substantially all of my `delta.com` browser window. (Screenshot.)

Like ordinary "adware" popup ads served by Claria and WhenU, the Hawaiian Airlines ad (as served by 180solutions) covers competitors' sites. But whereas Claria and WhenU popups generally cover only a portion of a site, this 180solutions popup for Hawaiian covers substantially all of `delta.com`.

In my initial testing of the 166,246 trigger words and phrases in 180's trigger database, I have found at least 8,000 triggers that are currently associated with pop-up advertisements. However, since the focus of this article is 180's effect on affiliate commissions, I omit a listing of all targeted triggers and their corresponding advertisements. Such data is available on request. I also have on hand videos, screen-shots, and network transmission logs showing the Hawaiian Airlines ad covering `delta.com`, as well as showing a large number of similar occurrences as to other advertisements and other targeted sites.

According to recent statements by 180 staff -- offers made in unsolicited emails (1, 2, 3, 4, 5, 6) -- 180 advertisers pay 180 as little as $0.015 (one and a half cents) per display of their ads using 180's software.

Some domains are ineligible for targeting by 180, because they have been placed in 180's "domain exclusion list." See my analysis of 180's exclusion list.

180's Actions and Their Effects on Affiliate Commissions [Affiliate data replacement via "double" windows | Silent replacement without the use of popups] Return to top

My testing identifies two distinct 180 practices that cause 180 to receive affiliate commissions. First, 180 causes users' computers to open "double" windows of the merchants users visit, where the duplicate window is reached through affiliate links (details). Second, 180 opens hidden windows of merchants' sites reached through affiliate links (details). This section presents these two methods in turn, after first briefly reviewing the theory of affiliate programs.

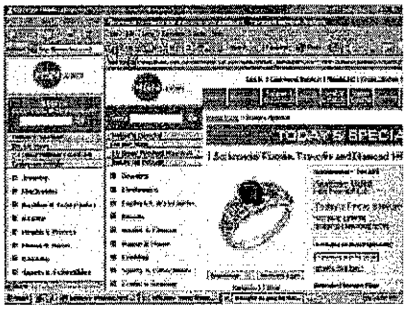
Review of Affiliate Programs Generally

The preceding section shows 180 displaying a near-full-screen web page of a competitor, targeting and covering the site a user had requested. But not all 180 ads are for competitors. Some 180 ads paradoxically promote the same merchant a user had initially requested. For example, when a user browses to `hsn.com` (the Home Shopping Network), 180 might cause the user's screen to show two browsers, both open to hsn.com -- the first browser (which the user had been using) along with an extra window (which 180 had opened).

To understand 180's decision to open a duplicate window to a given merchant, it is first necessary to review the general operation of online affiliate commission programs. These affiliate programs are designed to provide small payments to affiliate web sites who refer users -- ultimately, purchasers -- to online merchants. Affiliates offer users the ability to reach merchants' sites via special tracking links, and if users ultimately make purchases after clicking through these links, affiliates receive commission payments. Thus the usual affiliate process is as follows:

1. Affiliate web site creates pages that link to merchant via special tracking links.
2. User clicks on affiliate link to merchant.
3. User makes purchase.
4. Merchant tracks purchase and attributes it to the corresponding affiliate.
5. Affiliate receives payment from merchant according to merchant's contract with affiliate.

Affiliate code replacement via popup "double" windows



180 software intercedes in the affiliate commission process by changing users' tracking codes at certain online merchants. 180 software often makes this change by opening a second merchant window, using a 180 (or 180 advertiser) affiliate link to the merchant's web site, so as to replace the user's initial tracking data (if any) with 180's tracking codes. Via this "cookie-stuffing" technique, when a merchant attempts to determine which affiliate (if any) deserves credit for a user's purchase, the merchant sees the 180 affiliate codes. The merchant ultimately pays commission to 180 (or a 180 advertiser), rather than paying commission to the actual originating affiliate (if any) and rather than retaining commission fees (if the user arrived at the merchant's site without clicking through any affiliate).

The resulting on-screen display is as shown at right (screenshot). Shown below are the associated communications between 180's server and 180 software installed on my test PC.

keyword trigger

```
GET /showme.aspx?keyword=.hsn.com+hsn.com&did= ...
...

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<HEAD>
<meta name="vs_targetSchema" content="http://schemas.microsoft.com/intellisense/ie5">
</HEAD>
<body>
```

116 of 155

```
ncase_ad_url: <input id=ncase_ad_url name=ncase_ad_url
value=http://service.bfast.com/bfast/click?
bfmid=37919329&amp;siteid=...&amp;bfpage=hsncom_ts>
...
```

ad to be shown

The `service.bfast.com` URL tracks the fact that a user was sent from 180 to the merchant at issue. After recording this referral, the `bfast.com` server quickly redirects the user to the `hsn.com` site. (Note that I have removed the `siteid=` parameter which gives one of 180's affiliate codes for affiliate links via the Commission Junction affiliate network.)

Whether the user ultimately makes a purchase from the original web browser or from the 180 popup, 180 receives affiliate commission for the sale. This result occurs due to the "last-set-cookie-wins" effect, whereby one affiliate's cookie overwrites any prior affiliate's cookie. Cookies are shared by all active browser windows, so even a cookie set by the 180 popup browser nonetheless affects the original browser.

`hsn.com` is one of many merchants targeted with these double popup windows. In my testing (mimicking the transmissions made by 180 client software and observing the responses of 180's targeting server), at least 183 merchants are targeted with affiliate link popups that display in "double" windows like the `hsn.com` display shown above.

Merchants targeted with own affiliate links, displaying in "double" popup windows
(212 trigger conditions)

Available on request, I have videos, screen-shots, and network transmission logs showing 180's interference with the HSN site as shown above. I have similar records as to a large number of similar occurrences affecting other targeted sites.

NEW - Added by request (July 23 to October 17), ten examples of the behavior described above:

1. Extended packet log and video showing 180 communications and targeting substantially similar to those shown above, but targeting Gateway (a Commission Junction merchant) on July 23.
2. Extended packet log and video showing 180 communications and targeting of store.apple.com (a LinkShare merchant) on July 22.
3. Extended packet log and video showing 180 targeting The Golf Warehouse (tgw.com, a LinkShare merchant), when reached through an affiliate link on July 24.
4. Video and screenshots showing 180 targeting The Golf Warehouse on August 2.
5. Extended packet log and video showing 180 targeting FogDog (a Commission Junction BFAST merchant), when reached through an affiliate link on July 24.
6. Extended packet log and video showing 180 targeting Freshpair (a Commission Junction qksrv merchant), when reached through an affiliate link on July 27.
7. Extended packet log and video showing 180 targeting ValueMags (a Performics merchant), when reached through an affiliate link on July 24.
8. Extended packet log and video showing 180 targeting LillianVernon (a LinkShare merchant) on October 7.
9. Extended packet log and video showing 180 targeting MotherWear (a Commission Junction qksrv merchant) on October 7.
10. Extended packet log and video showing 180 targeting Crucial.com (a Commission Junction qksrv merchant) via a "obfuscated decoy" affiliate frameset on October 17.

Silent affiliate code replacement without the use of popup windows

Not all 180 "cookie-stuffing" requires showing a duplicate window of the merchant's site. Some 180 cookie-stuffing uses hidden windows -- opened off-screen via IFRAMEs and similar methods -- to create or replace users' affiliate tracking codes without causing an extra window to be opened on the user's screen. Such an approach is implemented via instructions -- from 180's servers to 180 software on users' PCs -- of form shown below:

```
GET /showme.aspx?keyword=.rei.com+rei.com&did=...
...

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<HEAD>
<meta name="vs_targetSchema" content="http://schemas.microsoft.com/intellisense/ie5">
```

keyword trigger

```
</HEAD>
<body>
<iframe src="http://click.linksynergy.com/fs-bin/click?
id=...&offerid=20594.10000191&type=4&subid=0"></iframe>
ncase_ad_id: <input id=ncase_ad_id name=ncase_ad_id
value=266410><BR>
ncase_keyword_id: <input id=ncase_keyword_id name=ncase_keyword_id value=172482><BR>
ncase_ad_windowtitle: <input id=ncase_ad_windowtitle name=ncase_ad_windowtitle
value="Brought to you by the Zango Search Assistant"><br>
<INPUT ID=kw_exclude TYPE=text style="VISIBILITY: hidden;" VALUE="%
3dwsi+empty+keyword+mailbox"><br>
<INPUT ID=ad_shown TYPE=text VALUE="y" style="VISIBILITY: hidden;"><br>
<SPAN class="957085619-06032003"><FONT face="Arial" color="#ff0000" size="5">Thank you

for your patience.&nbsp; You will be redirected to your destination site in a
few seconds.</FONT></SPAN>
</body>
</HTML>
```

embedded reference to ad to be rendered off-screen, not shown to user

The `click.linksynergy.com` URL tracks the fact that a user was sent from 180 to the merchant at issue. After recording this referral, the `linksynergy.com` server quickly redirects the user to the `rei.com` site. (Note that I have removed the `id=` parameter which gives one of 180's affiliate codes for affiliate links via Linkshare.)

In the course of events described in this section, there exists no notable on-screen image to be captured in a screenshot, and I therefore can provide no screenshot of this finding. Notwithstanding the lack of on-screen confirmation, my network monitoring confirms that the IFRAME at issue (definition) is rendered off-screen. My testing further confirms that the IFRAME overwrites users' cookies via the specified HTTP request to linksynergy (or, for some trigger conditions, other affiliate tracking services): I have confirmed such overwriting by observing that the IFRAME URL is requested by the user's PC, and that the user's cookies are altered accord to instructions in the corresponding HTTP response. As a result, commission flows to 180solutions without users ever receiving any on-screen indication that any commission transfer is taking place.

NEW - Added by request (July 20): Video of the web browsing that led to the transaction above (WMV format; view in Full Screen mode for best quality). Extended packet log of 180 communications in the transaction above.

Beyond IFRAMEs, 180 also uses certain JavaScript code to accomplish substantially the same result -- loading affiliate tracking pages in hidden windows so as to set or replace affiliate codes, again without alerting the user to what is taking place.

`rei.com` is one of many merchants targeted with silent affiliate code replacements. In my testing, at least 170 merchants are targeted with silent affiliate link replacement.

Merchants targeted with silent affiliate code replacement
(170 trigger conditions)

As to at least two merchants -- Dell and eBay -- 180's silent affiliate code replacement is particularly pronounced. For these merchants, 180's affiliate code replacement not only operates silently, but the replacement also proceeds only after a randomized delay. As a result, observing 180's affiliate code replacement for these merchants requires particularly careful network monitoring. Nonetheless, on multiple occasions I have observed and confirmed 180's activities as to these merchants, using the network monitoring method described above. I do not know why 180 made efforts to include a randomized delay, but one reasonable inference is that such a delay was thought to hinder detection by the merchants.

I have tested requests for targeted merchant sites after first browsing to affiliate sites and, from these affiliates, clicking through to the merchants at issue. I have observed that 180's behavior is unaffected by the presence of existing affiliate codes. Notwithstanding the fact that users may have recently viewed other affiliate sites which set affiliate tracking codes of their own, 180 proceeds with the double windows, IFRAMEs and other hidden windows as described above, overwriting other affiliates' tracking codes in the process. In addition, in at least some instances, 180 software specifically targets its pop-ups at affiliates' origination pages (the pages from which affiliates link to merchants) -- further interfering with tabulation of affiliate commissions.

The above results primarily come from testing of June 25-28, 2004. 180 is fully capable of modifying its behavior at any time. In fact, in early July, most hidden 180 targeting seems to have been suspended, at least temporarily. 180's decision to scale back its silent targeting may result from a recent announcement from LinkShare that LinkShare is investigating 180's activities. Alternatively, the suspension may be in response to my recent posting generally describing this forthcoming research, or in response to concerns from affiliate merchants, affiliates, or others. Nonetheless, in my testing, 180's "double" popups continue to target multiple merchants, including merchants using both LinkShare and Commission Junction. In addition, at least 20 merchants remain targeted by 180's silent affiliate code replacement -- including merchants using both LinkShare and Commission Junction. In my most recent testing, some affiliate links are hidden behind multiple layers of sequential redirects as well as complex JavaScript obfuscation and encoding.

Notwithstanding 180's recent changes, I have preserved ample documentary evidence of my findings. Available on request, I have network transmission logs showing 180's interference with many of the merchants discussed in this section, and a large number of other sites.

Discussion [Affected groups | Affiliate network response and delay | Merchant / affiliate response | Hindering detection | Fraud detection] Return to top

The five groups affected by 180 "cookie-stuffing"

180's cookie-stuffing affects five distinct groups, in the following ways:

1. *Users suffer from 180solutions' activities.* Users' affiliate commissions do not reach the affiliate (if any) that 180 users selected intentionally (e.g. to support a particular web site) or implicitly (e.g. by using that site and clicking through its links to recommended merchants). This redirection harms users -- especially when they are thwarted in their explicit goal of directing commissions to particular affiliates. To the extent that 180's activities take money from merchants, and merchants ultimately increase their prices to cover their costs, users -- even users without 180 software -- indirectly fund 180.
2. *Legitimate affiliates suffer from 180solutions' activities.* Legitimate affiliates lose commissions on purchases by users with 180 software installed. These losses are particularly serious to the extent that affiliates rely on these commissions -- e.g. to support their web hosting and development costs, or to make web publishing a job rather than a hobby.
3. *Merchants suffer from 180solutions' activities.* Merchants suffer in at least two distinct ways from 180's activities.
   a. 180 cookie-stuffing causes merchants to pay commissions to 180 even when users reached a merchant's site directly or through some source other than an affiliate link. If a user typed in a domain name after (for example) seeing an ad on TV or in print, the merchant has already "paid for" acquisition of that user via the offline advertising. If a user arrived at a site via a sponsored link from a search engine, the merchant incurs a cost for that user's visit via payment to the search engine. Nonetheless, 180's affiliate cookie-stuffing causes the merchant to pay *again* -- to pay *twice* for a single user and a single purchase. 180 cookie-stuffing therefore increases the cost of acquiring new customers, reducing the returns to merchants' advertising both online and offline.
   b. 180 cookie-stuffing causes merchants to pay commissions to 180 even when commission is properly payable to another affiliate. By reducing the earnings of other affiliates, 180's activities cause merchants to lose affiliates or to recruit worse or fewer affiliates. This in turn reduces the effectiveness of the merchant's overall affiliate program.
4. *180solutions benefits from 180solutions' activities.* Cookie-stuffing earns income for 180solutions. Indeed, in November 2003, MSNBC reported that during September 2003, 180 had earned more than $100,000 in commissions from more than $4 million of purchases at Dell. Now that 180 reports an installed base roughly twice as large, 180's earnings could be twice as large -- from Dell alone. At Dell's maximum commission rate of 4%, 180 makes a $40 commission on a $1000 PC -- meaning 180 stands to make a large amount of money if only a few thousand 180 users buy new computers each year. Furthermore, since 180 participates in several hundred affiliate programs, as described above, 180's actual affiliate earnings could be two orders of magnitude larger.
5. *Affiliate networks benefit, at least initially, from 180solutions' activities.* Affiliate merchants ordinarily pay their affiliate networks a percentage of all affiliate revenues passing through the network. So, the more money passes through the network -- including to 180solutions -- the more money affiliate networks make. Details below: Possible responses by affiliate networks, Delays in response by affiliate networks..

Possible responses by affiliate networks

When affiliate networks find evidence than an affiliate is violating network policies, affiliate networks can exclude that affiliate from future participation in the entire network (and all its merchants). Such exclusion is not unprecedented: For example, LinkShare excluded WhenU in March 2003. WhenU has subsequently remained absent from the LinkShare network.

In the two sections below, I present the relevant network policies for LinkShare and Commission Junction, the two largest affiliate networks.

Linkshare

The LinkShare Shopping Technologies Addendum (PDF) describes permissible behavior for LinkShare affiliates. The Addendum requires, in relevant part, that:

> "(i) No Affiliate Application will replace, intercept, interfere, hinder, disrupt or otherwise alter in any manner the Web user's access, view or usage of, or other aspect of the Web user's experience at, any Network Affiliate Webpage or in relation to any Destination Webpage (both as defined below) in a manner that causes or otherwise results in a different experience from what was otherwise intended by such third party Network Affiliate;" and

> "(ii) No Affiliate Application will block, alter, direct or redirect, or substitute, insert or append itself to, or otherwise intercept or interfere in any manner with, any click through or other traffic-based transaction that originated from a Network Affiliate Webpage in relation to a Destination Webpage as intended by the Network Affiliate (including without limitation any return visit to the Network Merchant to which such click through or other traffic reached or intended to reach) with the result of reducing any compensation or other payment earned by or owing to a third party."

In my inspection of 180 software, 180 violates provision (i) with its popup ads that cover affiliate networks and merchants, as shown above (consistent with the Hawaiian Airlines example). In my inspection of 180 software, 180 violates provision (ii) with its "double" popups and with its silent popups -- both of which alter, direct, redirect, substitute, and insert 180 affiliate codes where other affiliates' codes were present.

Accordingly, I believe LinkShare could terminate 180's participation in the LinkShare network for violation of the rules set forth above.

However, at present, 180 remains in LinkShare's network. I have spoken with multiple LinkShare merchants who tell me (on condition of anonymity) that their contacts at LinkShare insist 180 is in compliance with LinkShare's requirements. Furthermore, 180 staff have stated "Our Linkshare account is in compliance with the manners in which they allow affiliates to do business."

Commission Junction

The Commission Junction Publisher Service Agreement describes permissible behavior for Commission Junction affiliates. The Agreement requires, in relevant part, that:

> "You shall not cause any Transactions to be made that are not in good faith, including, but not limited to, using any device, program, robot, Iframes, hidden frames, redirects ..."

As shown in my network monitoring analysis above, 180 uses IFRAMEs, which Commission Junction's Agreement specifically defines to be in bad faith, and which the Agreement therefore prohibits. In addition, 180's "double" popups are caused by software installed on users' PCs, which I believe fits the definition of "device, program, robot" within the meaning of the Agreement. Finally, a strong case can be made of bad faith (again, prohibited by Commission Junction's Agreement) as to the totality of 180's system of causing merchant traffic to appear to originate through 180 affiliate links, when in fact it did not so originate.

The Commission Junction Publisher Code of Conduct specifies further requirements for Commission Junction affiliates. The Code requires, in relevant part, that:

> "No Web publisher ... or software download technology provider ... may interfere with or seek to influence improperly the referral of a potential customer or visitor ... to the Web site of an online advertiser ... No Publisher or Technology Provider will automatically replace or alter any component of a Service Provider's technology that results in a reduction of any compensation earned by another Publisher."

> "Altering another Publisher's site. Publishers may not alter, change, substitute or modify the

content of or appearance to an End-User of another Publisher's Web pages, use that Publisher's content to obtain an End-User referral, or obstruct access to another Publisher's Web pages (regardless of receiving permission from the End-User)."

In my inspection of 180 software, 180 interferes with the referral of customers to web sites by automatically overwriting tracking cookies, reducing the compensation earned by other affiliates. As such, 180 software violates the first provision above.

In my inspection of 180 software, 180 alters the appearance of web pages (including CJ publisher pages) as viewed by end users, because 180 shows popups that cover such pages, as shown above (consistent with the Hawaiian Airlines example).

Accordingly, I believe Commission Junction could terminate 180's participation in the Commission Junction network for violation of the rules set forth above -- in both the Publisher Service Agreement and the Code of Conduct.

However, at present, 180 remains in the Commission Junction network. See also a report stating that CJ gives 180 its highest ranking, and a message from CJ staff stating that 180 is in compliance with CJ rules.

This article is not the first to suggest that 180 violates CJ's rules. See prior discussion: 1, 2, 3.

Other affiliate networks

Certain other affiliate networks have already addressed 180's participation in their networks. In January 2004, Shareasale reported that not only had it previously removed 180 from its affiliate network, but it had also taken steps to stop 180 advertisers from receiving Shareasale commissions.

British affiliate networks have seemingly been particularly inclined to remove 180. 180 has been removed from the affiliate networks of Affiliate Future (November 2003), Paid On Results (November 2003), Affiliate Window (February 2004), Buy.at (February 2004), dealgroupmedia (April 2004) and the UK subsidiary of Commission Junction (May 2004).

In response to my research and to others' subsequent testing, affiliate network kowabunga.com sent its merchants an email that concluded, with regards to 180's activities, that: "these practices not only cheat your other affiliates, they cheat you [merchants] directly."

Delays in response by certain affiliate networks

Affiliate merchants ordinarily pay their affiliate networks a percentage of all affiliate revenues passing through the network. For example, Commission Junction's public pricing list reports that CJ charges a merchant 30% of all amounts to be paid to affiliates. (In other words, if a merchant sells $1,000,000 of merchandise and pays a 5% affiliate commission, then it must pay $50,000 of commission to its affiliates. It must further pay 30% of $50,000, or $15,000, to Commission Junction.)

As a result, in the first instance, affiliate networks benefit from cookie-stuffing of the sort that 180 performs. Such cookie-stuffing increases the total volume of sales flowing through affiliate networks (effect 3.a. above), and increases the affiliate commissions on which, for example, CJ can charge a 30% fee. Set against this short-run incentive is the long-term problem that if affiliate networks fall greatly in value to merchants, or if affiliate networks are perceived to facilitate fraud, then merchants may no longer be willing to pay affiliate commissions and affiliate network fees. But in the short run, affiliate networks benefit from more money flowing through their networks.

In this context, it is worthwhile to investigate the diligence with which affiliate networks have investigated 180's activities. 180's affiliate replacement behavior has been publicly known since at least MSNBC's November 20, 2003 report (based on interviews with 180 staff) of 180 receiving a share of purchases at Dell. Furthermore, allegations of fraud by 180 have been prevalent on online discussion boards frequented by affiliate network staff. See, for example, ABestWeb's 180solutions forum, where merchants were beginning to learn of 180's affiliate replacement activities in December 2003 or earlier. During spring and early summer 2004, I personally notified staff at Commission Junction and LinkShare of 180's violations as determined by my first-hand research. Nonetheless, as of the publication of this article in July 2004, 180 remains in the affiliate programs of both Commission Junction and LinkShare.

Some affiliates have suggested that affiliate networks allow 180solutions to stay in their networks because ejecting 180 would cause the networks to lose revenue. (1, 2, 3, 4, 5, 6)

Some affiliates, affiliate merchants, and other discussants have reported that affiliate network staff (including staff from Commission Junction and LinkShare) have recommended 180solutions (and similar programs) as a valuable addition to their affiliate programs. See e.g. a report of CJ giving 180 its highest ranking, a message from CJ staff stating that 180 is in compliance with CJ rules, and a message reporting CJ staff promoting browser helpers to merchants. A further message explicitly points out networks' conflict of interest between increasing their own revenue and serving their merchants. Two further messages (1, 2) complain that CJ "made no attempts to explain" and "never [provided] any information about" the practices of programs installed on users' PCs that tamper with affiliate tracking systems. On condition of anonymity, multiple Linkshare merchants have told me that their contacts at LinkShare also speak highly of 180. So far as I know, LinkShare staff issued no public response to 180's claim that "our Linkshare account is in compliance with the manners in which they allow affiliates to do business."

LinkShare recently posted an announcement stating that it is reviewing 180's participation in the LinkShare network. However, pending completion of LinkShare's evaluation, LinkShare staff state that LinkShare is allowing 180 to remain in its program.

Merchants are damaged significantly and irreversibly by networks' delays in responding to 180's affiliate code replacements. Even if 180's transactions are subsequently reversed, merchants will have issued checks to 180 for prior months' commissions. Merchants may have difficulty retrieving these amounts from 180 retroactively.

Affiliates are also damaged significantly and irreversibly by networks' delays in responding to 180's affiliate code replacements. Once affiliate codes are overwritten with 180's codes, they cannot readily be restored. (I have drafted some initial methods to restore some affiliate commissions using affiliate networks' web server log file data, but my methods are difficult and only work under certain circumstances.) As a result, delays in addressing 180's behavior mean irreversible (or substantially irreversible) loss of commissions to affiliates who comply with networks' rules.

Possible responses by affiliate merchants and ordinary affiliates

Affiliate merchants can exclude an affiliate from their respective programs. Online discussions report that some merchants have already excluded 180. Such merchants include Alibris, British Airways, Overstock.com, Western Union, GSICommerce (on behalf of multiple merchants including Kmart, Modell's, Reebok, Sports Authority, and Tweeter), Coldwater Creek, and Surplus Computers.

Although affiliate merchants are harmed when 180 seizes affiliate commissions, in certain circumstances merchants' affiliate manages may nonetheless have an incentive to let the harm continue. Consider a merchant affiliate program manager whose salary, prestige, or other compensation turns on the size of the merchant's affiliate program. If the merchant affiliate program manager excludes 180 from the merchant's affiliate program, then the program will seem to shrink -- reflecting that no affiliate commission will be paid on sales not originating at bona fide affiliates. This change is in the merchant's best interest, since it saves the merchant money on commissions that need not be paid. However, the change is (by hypothesis) contrary to the affiliate manager's self-interest. This factor is likely to be particularly pronounced as to merchants who outsource the management of their affiliate programs. (Details in affiliatemanager.net forums - registration required.)

Ordinary affiliates have no direct ability to affect 180 or to protect their commissions from being seized by 180 software. An affiliate's direct responsibility ends with providing a web page that correctly links to an affiliate tracking network, and affiliates have no direct way to tell what happens subsequently. Affiliates have no ability to directly observe whether merchants correctly credit affiliates for all clicks, whether merchants correctly credit affiliates for all purchases resulting from those clicks, or whether software such as 180 intercedes in such transactions and overwrites the first affiliate's cookies. As such, in important respects, affiliates must rely on -- must hope for -- the good faith, correct design, and rigorous policy enforcement of affiliate networks and affiliate merchants.

180 practices that hinder detection exclusion from affiliate programs

180 designs its software and systems in multiple ways that make it difficult or impossible to fully study 180's activities, and to track all affiliate accounts used by 180 and its advertiser partners. These practices include the following:

1. Redirecting affiliate commissions without any on-screen display whatsoever. If 180's software showed even a small temporary message on screen (a one-second alert that "commission for your purchase will go to 180solutions"), affiliate merchants and interested users would far more easily be able to identify 180's behavior.

2. Using multiple affiliate accounts under different names, and allowing 180 advertisers to add their own affiliate codes to 180's system. In my examination of 180 configuration files, I can see that 180 currently causes users' computers to invoke at least 13 distinct LinkShare accounts and at least 71 distinct Commission Junction accounts (25 for bfast and 46 for qksrv). I gather that some of these affiliate accounts are held by 180 advertisers, rather than by 180 itself; but in as much as all the codes are served through 180 software, via methods including those described above, they all pose the same problem for merchants: Because 180 software uses so many affiliate codes, not all labeled with 180's corporate name, merchants have no easy way to block all affiliate traffic coming from or through 180. (Complaints about multiple 180 accounts: 1, 2, 3, 4)
3. Redirecting affiliate traffic through multiple domains. The examples shown above include direct bfast and linksynergy links in 180 server instructions to 180 software as installed on users' PCs. But my testing shows that 180 affiliate code traffic often passes through one or more redirect servers. One particularly prevalent such server is shoptoday.us, though I have found traffic passing through dozens of other servers. (Details available on request.) Again, 180 advertisers (rather than 180 itself) may be responsible for some or many of the redirections, but from the perspective of merchants, the problem is identical whether initiated by 180 itself or by 180 advertisers.
4. Using "private registrations" (such as Network Solutions Private Registrations) to shield Whois data, to avoid disclosing the true registrant of the redirect domains described in #3. See screenshot.

As a result, even if affiliate merchants learn what 180 is doing and even if merchants seek to remove 180 from their affiliate programs, it is particularly difficult for merchants to find the many affiliate IDs used in 180 advertisements, and to exclude all such affiliate IDs.

All this said, network monitoring generally allows me to find all affiliate ID numbers used in 180 advertisements, no matter how many affiliate IDs 180 obtains and no matter how many levels of redirects hide each affiliate's ID number.

Approaches to fraud detection

To date, detection of affiliate fraud has taken place in ways that are best described as uncoordinated:

> If affiliate networks operate fraud detection programs, they seem to be understaffed or ill-equipped to deal with the fraud currently taking place. I draw this conclusion from slow or nonexistent responses to date, even as to large commission redirection systems such as 180's.
>
> Some merchants attempt to detect fraud against their affiliate programs, independent of any fraud control efforts at affiliate networks. But merchant-by-merchant investigation creates widespread duplication of effort: Scores of merchants have to investigate each alleged case of fraud, without any effective way to share their findings or coordinate their efforts. Furthermore, since detecting sophisticated affiliate fraud requires specialized skills and, to some extent, specialized hardware and software, most merchants are unlikely to have the necessary resources on hand.
>
> Discussions among affiliates, e.g. in ABestWeb Forums, often consider the problems of affiliate fraud -- and the negative effects on the affiliates who make up the bulk of ABW participants. But even when ABW participants find evidence of fraud, it is difficult to get this information to the right decision-makers at merchants and networks -- again, for lack of any centralized or official information dissemination apparatus.

Having reviewed this state of affairs, I believe it to be a recipe for bad outcomes -- for widespread fraud with few meaningful attempts at prevention, with merchants and legitimate affiliates suffering the consequences.

I do not aspire to serve as a fraud detector as to all affiliate programs everywhere, or as to all affiliate fraud everywhere. However, I do intend to continue research in this field. Merchants seeking help with fraud detection may contact me or join my fraud detection mailing list for occasional announcements of new research in this area.

For those seeking to investigate affiliate fraud, my primary current recommendation is to go beyond watching what appears on screen on ordinary testing PCs. For "traditional" affiliate fraud schemes, ordinary PCs were sufficient -- for fraud would have telltale signs in on-screen displays or in HTML code readily viewed via View-Source or similar. But when affiliate code replacement is silent, as in the 180 efforts shown above, testing staff cannot know whether fraud has taken place merely by looking at the PC screen. Instead, full analysis requires network traffic analysis, of the sort described in my methodology section and shown above.

Responses from 180solutions, Affiliate Networks, Affiliate Merchants, Affiliates

In this section, I will post or link to responses I receive from 180solutions, affiliate networks, affiliate merchants, and affiliates.

On June 29, LinkShare announced that it is reviewing 180's participation in the LinkShare network. However, pending completion of LinkShare's evaluation, LinkShare's announcement reports that LinkShare is allowing 180 to remain in its program.

On July 9, a reporter following this story told me that his contact at LinkShare stated that LinkShare has "revised" its contract with 180solutions "because of complaints from affiliates and merchants." Nonetheless, in my testing, "double" popups continue to target multiple LinkShare merchants.

On July 10, a 180 staff person posted a response to my research on ABestWeb forums. Among other claims, 180 suggests that its use of affiliate popups -- both "double" and "silent" was to "protecting our customer's site from competing advertisers" and to "improve the shopper's experience." I posted a lengthy point-by-point critique of 180's claims -- including pointing out that using affiliate codes other than "with the intention of deliving valid sales leads" is contrary to LinkShare terms and conditions; noting that 180 can better protect merchants and serve shoppers by showing no popups and by tampering with no affiliate codes; and observing out that 180 benefits financially from the affiliate code tampering I have documented.

On July 12, 180 issued a press release reporting that it "will retain one of the nation's top independent audit firms to review its affiliate marketing practices."

On July 13, a 180 staff person was quoted as claiming that "LinkShare has embraced 180Solutions' deployment of double and hidden pop-ups."

On July 14, I observed that 180 has modified the config.aspx file on its web server to specifically exclude 71 domains, including cooking.com, dell.com, ftd.com, sharperimage.com, register.com, walmart.com, and numerous others. These are major additions beyond 180's prior "exclude list" as I have previously observed it. Nonetheless, scores of other merchants (itemized on the lists linked above) remain targeted. See my subsequent analysis of 180's exclusion list.

On July 15, 180 staff was quoted in MediaDailyNews as claiming that it "does not incur any revenue from its deployment of double and hidden pop-ups." 180 further claimed that the hidden pop-ups are "devoid of any tags or codes that redirect to 180solutions or its advertisers." This claim is specifically contrary to my finding above, showing affiliate links within 180 IFRAMEs. 180 claims that "empty i-frames are the only way to avoid the automatic deployment of another company's ad," but my research has found multiple other methods by which 180 can and does avoid the deploment of other ads -- including "No Ad Available" responses from 180 servers to its software, and including hidden IFRAMEs that truly are blank. Finally, 180 claims that it only uses double pop-ups with Commission Junction's network, and hidden pop-ups with LinkShare's network -- but I have found instances of the hidden pop-ups targeting CJ merchants and double pop-ups targeting LinkShare. See also my point-by-point response to this article.

On July 27, Commission Junction staff reviewed my research and concluded that "another publisher ... is doing ... overwriting" -- referring to my demonstration of a 180 advertiser ("another publisher" other than 180 itself) overwriting another affiliate's cookies.

The above results primarily come from testing of June 25-28, 2004. 180 is fully capable of modifying its behavior at any time. In fact, in early July, most hidden 180 targeting seems to have been suspended, at least temporarily. 180's decision to scale back its silent targeting may result from LinkShare's announcement that it is investigating 180's activities. Alternatively, the suspension of hidden targeting may be in response to my recent posting generally describing this forthcoming research, or in response to concerns from affiliate merchants, affiliates, or others. Nonetheless, in my testing, 180's "double" popups continue to target multiple merchants, including merchants using both LinkShare and Commission Junction. In addition, at least 20 merchants remain targeted by 180's silent affiliate code replacement -- including merchants using both LinkShare and Commission Junction. In my most recent testing, some affiliate links are hidden behind multiple layers of sequential redirects as well as complex JavaScript obfuscation and encoding.

I am currently planning widespread testing of more programs that may be redirecting or tampering with affiliate commissions. Interested merchants, please fill out this form to join my affiliate fraud detection list, so I can keep you up to date with updates.

Disclosures

Return to top

My interest in spyware originally arose in part from a prior consulting engagement in which I served as an expert to parties adverse to

Gator in litigation. See Washingtonpost.Newsweek Interactive Company, LLC, et al. v. the Gator Corporation.

More recently, I have served as an expert or consultant to other parties adverse to spyware companies, including parties generally contemplating litigation adverse to 180solutions. I have also attempted to assist several affiliate merchants as to affiliate fraud prevention. I continue to accept further engagements of this general form.

Finally, I have recently been in touch with staff of affiliate networks LinkShare and Commission Junction -- generally discussing the ways I might help these networks address, detect, and stop online affiliate fraud. However, to date I have accepted no relationship beyond phone calls with these or other affiliate networks.

This page is my own work - created on my own, without approval by any client, without payment from any client.

I gratefully acknowledge numerous helpful suggestions and assistance from Kellie Stevens, President of AffiliateFairPlay.

Last Updated: October 20, 2004 - Sign up for notification of major updates and related work.

Spyware Warrior is horrified to present...

180solutions in 365 Days

A year in the life of an adware company...

What we learned about 180solutions (*aka* Zango & MetricsDirect) during the year 2005:

1. 180 was caught by-passing its own notice & disclosure prompts during installation of its software

http://sunbeltblog.blogspot.com/2005/03/180-solutions_111084184539001994.html
http://netrn.net/spywareblog/archives/2005/04/09/oh-what-a-tangled-web-we-weave/

2. 180 was caught disseminating demonstrably false & misleading information about its practices to the public

http://netrn.net/spywareblog/archives/2005/04/03/scratch-a-lie-find-a-thief/

3. 180's software was repeatedly caught being illegally or deceptively installed on web surfers' PCs

http://www.benedelman.org/news/100505-1.html
http://www.benedelman.org/news/050205-1.html
http://www.benedelman.org/spyware/installations/pacerd/
http://www.benedelman.org/spyware/installations/3d-screensaver
http://www.webhelper4u.com/nontransponders/wallpapers4u_4022005.html
http://www.spywarewarrior.com/adw2005/adw2005_1.htm#inst_180
http://www.spywareguide.com/articles/anatomy_of_a_drive_by_install__72.html
http://www.kephyr.com/spywarescanner/pus-practices/index.phtml#lookoutsoft.net-2005-11-11
http://www.kephyr.com/spywarescanner/pus-practices/index.phtml#pacimedia.com-2005-10-05
http://www.kephyr.com/spywarescanner/pus-practices/index.phtml#behost.biz-2005-09-27-part2
http://www.kephyr.com/spywarescanner/pus-practices/index.phtml#highconvert.com-2005-08-17
http://www.kephyr.com/spywarescanner/pus-practices/index.phtml#highconvert.com-2005-08-11
http://www.kephyr.com/spywarescanner/pus-practices/index.phtml#imbuddy-2005-08-06
http://www.kephyr.com/spywarescanner/pus-practices/index.phtml#aimface-2005-08-05
http://www.kephyr.com/spywarescanner/pus-practices/index.phtml#iowrestling.com-2005-06-30
http://www.kephyr.com/spywarescanner/pus-practices/index.phtml#crazy-toolbar.com-2005-06-16
http://www.kephyr.com/spywarescanner/pus-practices/index.phtml#ebs.fuck-access.com-2005-06-14
http://www.kephyr.com/spywarescanner/pus-practices/index.phtml#imbuddy.net-2005-04-13
http://www.kephyr.com/spywarescanner/pus-practices/index.phtml#aimface-2005-04-12
http://sunbeltblog.blogspot.com/2005/11/seen-in-wild-lookoutsoftnet.html
http://sunbeltblog.blogspot.com/2005/09/whats-wrong-with-this-picture.html
http://sunbeltblog.blogspot.com/2005/09/180-answers-back.html
http://netrn.net/spywareblog/archives/2005/09/25/activex-the-good-the-bad-and-the-ugly/

4. 180's software was caught being installed through BitTorrent packages in a decidely underhanded fashion

http://www.vitalsecurity.org/2005/06/aurora-install-source-revealed-and-175.html

http://www.vitalsecurity.org/2005/06/180-solutions-go-to-pieces.html
http://www.pcpitstop.com/spycheck/badtorrent.asp

Note that some of those BitTorrent downloads included kiddie porn:

http://www.vitalsecurity.org/2005/06/why-underage-porn-is-bad-pr.html

5. 180 returned to the BitTorrent trough even after being exposed earlier

http://www.pcpitstop.com/news/dave/2005-07.asp
http://www.vitalsecurity.org/2005/07/180-solutions-and-cdt-take-train-to.html

6. 180 was publicly denounced for deceptive & fraudulent advertising distributed through its network

http://www.vitalsecurity.org/2005/05/180-solutions-down-for-count.html

More recently 180 was caught popping up sleazy ads over the Federal Trade Commission's web site:

http://netrn.net/spywareblog/archives/2005/11/17/does-180solutions-know-better-than-the-ftc/

7. 180's "re-notification" prompts were exposed as a sham

http://www.benedelman.org/news/062805-1.html

8. 180 pledged to stop distributing 3rd-party adware through CDT, Inc. (purchased in March 2005), only to renege on that promise later

The promise (Apr. 2005):
http://news.com.com/Deal+may+mean+shifting+adware+model/2100-1032_3-5660393.html

The reality (Nov. 2005):
http://eula.winadclient.com/general/
http://www.windupdates.com/license.html

9. 180's software was caught being illegally installed through IM exploits

http://www.revenews.com/wayneporter/archives/000883.html
http://www.spywareguide.com/articles/greynets_instant_messenger_ope_75.html
http://www.facetime.com/pdf/IMPactThreatDetail_VariantofW32SdbotAAH.pdf?Ref=spgpdf

10. 180's software was caught being installed by a site peddling kiddie porn and dropping spam zombies

http://sunbeltblog.blogspot.com/2005/08/spywarekiddie-pornspam-zombie.html
http://sunbeltblog.blogspot.com/2005/09/180-solutions-responds-to.html

11. 180's software was caught being mass-installed through illegal bot-nets

http://www.washingtonpost.com/wp-dyn/content/article/2005/08/16/AR2005081600727.html
http://www.wired.com/news/technology/0,1282,69480,00.html?tw=wn_tophead_2

http://blogs.washingtonpost.com/securityfix/2005/11/the_botnetspywa.html
http://www.theregister.co.uk/2005/08/16/180_sues_bad_actors/
http://news.com.com/Ad+software+maker+sues+distributors/2100-1030_3-5836884.html?tag=nefd.top

12. 180's distribution channels were so utterly compromised that 180 was blackmailed by one of its own distributors

http://informationweek.com/story/showArticle.jhtml?articleID=173402817
http://news.com.com/Adware+maker+We+were+victim+of+cybergang/2100-7349_3-5930099.html

13. 180 was hit with a class action lawsuit for multiple deceptive practices & "trespass to chattels"

http://blogs.zdnet.com/Spyware/?p=655
http://www.chicagotribune.com/news/local/southsouthwest/chi-0509140224sep14,1,3740205.story?...
http://publications.mediapost.com/index.cfm?
fuseaction=Articles.showArticleHomePage&art_aid=34089

14. 180's software was caught being deceptively installed by illegal crackz sites

http://www.kephyr.com/spywarescanner/pus-practices/index.phtml#crackz.ws-2005-06-11-nero
http://www.vitalsecurity.org/2005/09/ysbweb-serve-up-crack-extractor-whoops.html
http://sunbeltblog.blogspot.com/2005/11/seen-in-wild-adware-on-crack-sites.html

15. 180's software was caught being installed at kids sites

http://www.benedelman.org/spyware/installations/ezone-180/
http://netrn.net/spywareblog/archives/2005/11/13/180solutions-sponsors-class-of-second-graders-in-ohio/

16. 180 was forced to cough up a major distribution channel (IST) after being threatened by the Center for Democracy & Technology with an FTC complaint

http://blogs.washingtonpost.com/securityfix/2005/10/adware_purveyor.html
http://blogs.zdnet.com/Spyware/?p=674

17. 180 was banned or booted from several major advertising networks

http://itmanagement.earthweb.com/columns/executive_tech/article.php/3556856
http://www.lurhq.com/latimesadbucks.pdf (LA Times)
http://www.eweek.com/article2/0,1895,1830072,00.asp
http://www.revenews.com/jeffmolander/archives/000650.html
http://www.amwso.com/rss/detail.php?ID=4
http://www.affiliatetip.com/blog/archives/wayne_porter_vs_180solutions_in_a_steel_cage_match.html

18. Most recently, 180's software was caught being distributed via a rootkit-infested worm on IM channels

http://www.facetime.com/pr/pr051028.aspx
http://www.spywareguide.com/articles/worm_propogates_via_aol_im_ins_91.html
http://news.zdnet.com/2100-1009_22-5920403.html

http://www.revenews.com/wayneporter/archives/001110.html
http://www.revenews.com/wayneporter/archives/001230.html

...via sites associated with CoolWebSearch:

http://sunbeltblog.blogspot.com/2005/11/180-solutions-attacked-by-_113106344456479064.html
http://blogs.zdnet.com/Spyware/?p=693

...via a security exploit at a crackz site that also dropped a rootkit and spam zombie:

http://netrn.net/spywareblog/archives/2005/11/29/anti-spyware-zealot-rants-about-180solutions/
http://netrn.net/spywareblog/archives/2005/12/01/180solutions-responds-to-installation-at-crack-site/

...and at a site with "humorous" racist videos:

http://sunbeltblog.blogspot.com/2005/12/httpcastlecopscomp672607.html
http://blogs.zdnet.com/Spyware/?p=720
http://www.revenews.com/chrisboyd/2005/12/the_value_prop_of_comedic_raci.html

Last Updated: 11 Dec. 2005

© Copyright 2005 SpywareWarrior.com

SunbeltBLOG

A blog about activities, products and ideas at Sunbelt Software, one of the leading developers of security software to protect against spyware, spam and

MONDAY, MARCH 14, 2005

180 Solutions...

3/24 update here
3/14 updated

180 Solutions has been trying to become legitimate (see, for example, Wayne Cunningham's post on his blog). Their joining COAST (the antispyware consortium) was the primary reason COAST recently fell apart.

As a result of 180 Solutions contacting us, we followed up with our usual extensive analysis of their practices. However, during the analysis we discovered some other things. We have written a whitepaper that details the issues we found here.

The whitepaper will be released in a formal fashion over the next several days, but I thought I would give a bit of advance notice on the blog.

The evidence is not in 180's favor.

There's a lot in this writeup, but as Suzi at SpywareWarrior pointed out, the areas that are probably most interesting to people are on pages 9-10 and and 18-26.

Here's the quick and dirty:

As part of 180's COAST certification, 180 agreed to a "CBC Force Prompt". This feature is designed to alert users to the installation of 180's software.

This prompt is shown when a certain registry key is set to "0". If it's set to "1", there is no prompt.

This is a serious weakness in the 180 installer. It is trivially easy for a rogue affiliate to simply set the value to 1, and the 180 install sails through, with the end-user none the wiser.

However, it appears that 180solutions is itself electing to bypass the "CBC Force prompt" in order to avoid alerting users to the installation of 180's software, and the implications of this are serious.

Sunbelt observed several installations of older versions of the 180search Assistant in which that software was updated to the latest version. After older versions of the 180search Assistant were "stealth-installed" via a Windows Media Player file and via a Java applet at lyricsdomain.com, that software called out to 180's servers, and downloaded and installed the latest, COAST-certified version of the 180search Assistant.

This behavior is especially disturbing because many of the installations that 180solutions is silently updating through this method are the possible products of "force-installs" of 180's software of users' PCs, where those users received no notice or warning whatsoever of the 180search Assistant.

Instead of alerting users to the presence of 180's software on their systems, 180 is updating those older software installations and versions to the latest 180search Assistant, allowing 180 to continue deriving economic benefit from those installations, entirely contrary to its publicly stated intention to clean up its distribution channels.

Alex Eckelberry

POSTED BY SUNBELT SOFTWARE BLOG AT 6:10 PM PERMALINK

Spyware Warrior

Waging the war against spyware.

4/3/2005

SCRATCH A LIE, FIND A THIEF

A few days ago I published an interview with Jay Cross, former researcher for the Consortium of Anti-Spyware Technology Vendors, which got into hot water with the anti-spyware community and eventually collapsed after is granted membership to 180solutions. It seems that Jay Cross isn't the only one giving interviews these days. Wayne Porter just published an interview with 180solutions on his ReveNews blog. Wayne prefaces that interview with some thoughts of his own.

I strongly encourage everyone to read both pieces.

As I noted in an earlier blog entry, we've been waiting for 180's responses to Wayne's questions. It's particularly interesting now to get answers to Wayne's questio[illegible]as recently put on the hot seat by Sunbelt Software, which published a white pap[illegible]'s software and business practices. The white paper was later taken down at 180solutio[illegible]st.

Now that we have 180's answers, let's take a good hard look at them and see how well they reflect what we already know about the reality of 180solutions and how its software behaves.

Before diving in, let me point out that there is already quite a bit of information about 180 that's readily accessible on the web. Much of this valuable information comes from Ben Edelman, who has written several times on 180solutions:

180solutions Installation Methods and License Agreement

180 Talks a Big Talk, but Doesn't Deliver

The Effect of 180solutions on Affiliate Commissions and Merchants

Media Files that Spread Spyware

Who Profits from Security Holes?

Ben refuted a number of erroneous or misleading claims made by a 180 representative about its advertising in this discussion last summer at the ABestWeb forum.

Readers should also have a look at Andrew Clover's detailed write-up at doxdesk.com about nCase

With all the information out there about 180, it doesn't take a rocket scientist to figure out that the answers that 180 gave to Wayne's questions are deceptive, evasive, and full of spin. In many cases 180 doesn't even bother to answer the question that was actually asked. Instead, they go onto some pleasant-sounding PR tangent, probably hoping that no one will notice that they're not answering the questions. Even when they do answer, their language is so full of meaningless euphemisms and jargon that you practically need a knife to cut through all the B.S.

April 2005

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

« Mar May »

Search Blog

search

Spyware Warrior Recommended Books

Best Price $22.92
or Buy New $37.96
Buy from amazon.com
Privacy Information

So, let's take Wayne's twelve questions one-by-one and see what we get from 180...

Questions 1 & 2: COAST

Question 1 asks what promises 180 made to COAST to get admitted. 180 responds by making some noises about improving "user notification, consent, and uninstall capabilities" and making "changes to both the application and distribution channel." That's fine as far it goes, but they never do provide the specific details of their promises.

In Question 2, though, the heavy spin begins. Wayne asked why 180 is still publicly touting its membership in COAST when that organization collapsed, is no longer in operation, and has no credibility among experts and researchers in the anti-spyware community. 180 simply evades the whole point of the question, neither denying that it continues to brag about its COAST membership, yet never explaining why it's doing that.

It's quite clear at this point that 180 has always seen a public relations bonanza in the COAST admission, and has been eagerly flacking that membership ever since, even to other software vendors and advertisers who might not know that COAST collapsed. As Wayne noted in his question, Duane Jeffers reported that 180 was doing this at the "Game Developer's Conference" in San Francisco just a few weeks ago.

And until very, very recently, 180 had a banner on their web site announcing its admission into COAST (they took it down after Wayne submitted his questions to them). But it gets worse. Apparently 180 was bragging on its COAST membership in November, 2004 to a representative of the "Homepage-Host Group"—that's a full 2 months BEFORE it was actually actually admitted to COAST.

What's so funny about that communication with "Homepage-Host Group" is that the 180 rep goes out of his way to distance Zango from the 180search Assistant, pretty much admitting that the 180search Assistant (which is essentially the same application as Zango) is bad news.

As you can see, sometimes its takes a lot to cut through 180's spin.

Questions 3 & 4: nCase

Question 3 is fairly innocuous: it simply asked 180 to explain what happened to its old nCase software, which operated very similarly to the newer 180search Assistant and Zango Search Assistant.

Question 4, though, is a revealing followup to Question 3. It asks whether 180 notified users with the nCase software on their computers that the software was being upgraded to the 180search Assistant. It also asks **how** 180 notified those users that the software on their PCs was being upgraded.

The answer to this question is important because a lot of those nCase users might not have been willing users at all. The older nCase software was known to be stealth-installed on users computers, as Ben Edelman noted when he told the Seattle Post-Intelligencer last summer "N-Case is definitely installed without consumers' informed consent in many or most instances". Even Todd Sawicki of 180solutions admitted to the same Seattle PI reporter that stealth installs of 180's nCase software were going on.

> [Sawicki] said n-Case could get bundled with other free software programs without the company's knowledge. And that could lead to the n-Case software fastening to individual's computers without their knowledge, he said.

Archives
November 2006
August 2006
July 2006
June 2006
May 2006
April 2006
March 2006
February 2006
January 2006
December 2005
November 2005
October 2005
September 2005
August 2005
July 2005
June 2005
May 2005
April 2005
March 2005
February 2005
January 2005
December 2004
November 2004
October 2004
September 2004
August 2004
July 2004
June 2004
May 2004
April 2004
March 2004
February 2004

If the nCase software was being stealth-installed on people's PCs, 180 should have at least notified them when it "upgraded" the nCase software to the 180search Assistant. In fact, if 180solutions wanted to be completely ethical, it shouldn't have even "upgraded" the nCase installs at all – it simply should have abandoned them, knowing that a lot of them could have come from illegal force-installs.

So what did 180 do with those older nCase installs? Did it notify users? 180 pointedly refuses to address the critical questions put to them by Wayne. It simply provides this terse one line response to Wayne's excellent questions:

> We upgraded the users at the same time we introduced the new, easier uninstall process.

In other words, they did NOT notify users—they simply "upgraded" the software on users' computers without telling them. Why would 180 do that? Oh, maybe, because if 180 told users that annoying advertising software had been installed on their computers behind their backs, the users might get pissed off and remove it? Could that be the reason?

What 180 did with the old nCase installations is most revealing, as we shall see in just a bit, because 180 is currently engaged in very similar shenanigans—"upgrading" older versions of the 180search Assistant to the new "COAST-certified" versions without notifying users, despite trying to give the mistaken impression that it's doing everything above-board. The leopard never really changes its spots, does it?

Questions 5-8: Stealth-Installs

180's responses to Question 5-8 are so full of deceptive, misleading B.S., you'd need to write a Ph.D dissertation to fully refute them. I'll try to keep this simple and straightforward.

In question 5, Wayne asked about the stealth-installs of 180's software, whether those are still happening, and what 180 is doing to stop them. Instead of answering the questions in a straightforward manner, 180 attempts to give the impression that it is vigorously policing its distributors. It even mentions the "industry-wide distribution monitoring service as in part envisioned by Jay Cross," which Jay discussed in his interview with me a few days ago. (One question for Jay and 180: why was 180 admitted to COAST before this "monitoring service" was created to actually verify the changes that 180 promised to COAST? Why wasn't 180's behavior actually verified before it was admitted to COAST and before 180 started bragging to the world about its admission into COAST?)

What 180 never does, though, is answer the meat of the question: are stealth installs still happening? As anyone in the anti-spyware community can tell you, they are still going on. (Note this comment from yesterday on Sunbelt's blog.) Sunbelt Software reports that it told 180solutions that those stealth installs are still going on. (I know this from reading the Sunbelt white paper while it was still available from the Sunbelt blog.) So why doesn't 180solutions admit that? Perhaps because it would cast doubt on the effectiveness of 180's efforts to police distributors?

180 also tries to give the impression that it is scrupulous in recruiting distributors, but this just isn't so. As Ben Edelman has reported, 180 has been reckless in soliciting distributors through unsolicited commercial email (UCE, "spam"). Even Todd Sawicki of 180 admitted that 180 isn't completely familiar with or in control of all the people and web sites distributing its software when he attempted to distance 180 from those rogue distributors and claim 180 wasn't responsible for their actions. Sawicki told the Los Angeles Times last year that those distributors are "guys in Bermuda, offshore. They're the online equivalent of spammers". Just how scrupulous could 180 be in recruiting distributors if this is the result?

January 2004
December 2003

Recent Entries

Rob Martinson, Walt Rines and the FTC - final chapter
Movieland.com sued by Washington State AG for spyware
InterCage/Atrivo IP
CastleCops responds to
Stoller
Trademark Troll Leo Stoller targets CastleCops
Spyware fighter under attack by trojan from DollarRevenue
Gimmy some Cash and Dollar Revenue!
180solutions and
$4 million
180solutions at it again, this time with

135 of 155

Wayne's question 6 continues asking more about stealth-installs and what 180 is doing to stop rogue distributors. 180 again tries to give the impression of being pro-active in policing its distributors, but there are huge problems with that, as I just noted.

The more important part of 180's response comes when it claims that users of its new software are always given clear notice before installation. 180 says:

> First, we only distribute an installation file whose purpose is to verify a user's intent to install. Then once that consent has been confirmed through a prompt like the one below, the installer file will call to our servers and download the application. This will solve any going forward issues of old code circulating in various distribution channels as well as allow us to more tightly control our distributors.

Below that response is a screenshot of a "Example Prompt" displayed to users during installation.

For the moment, let's set aside the question of whether that prompt is always displayed when it should be and look at the actual language of the prompt itself. Let's see what kind of notice and disclosure that prompt actually provides. It reads:

> Easy Messenger lets you combine your AIM, MSN, Yahoo, and ICQ buddies into one convenient IM!
>
> Easy Messenger is powered by 180search Assistant, a program that helps conduct faster, more productive searches and helps keep online entertainment and downloads free and safe. When running, 180search Assistant can be accessed from an icon in your system tray. This program shows you an average of 2-3 keyword-based advertiser web pages daily.
>
> By selecting 'Finish' you agree to the Terms and Conditions of the end user license agreement.
>
> Download Easy Messenger for FREE now!

This is not much notice or disclosure. In fact, it's downright deceptive. "Powered by 180search Assistant" makes it sound like the chat software itself relies on 180search Assistant to actually connect users and allow them to chat. That's not true—180search Assistant is a separate advertising program, not part of the chat software itself.

In fact, 180 goes out of its way to avoid telling users what they really need to know—namely, that the 180search Assistant is an advertising program that will track their online surfing, transmit that information to 180, and pop up advertising on their desktops. But 180 never says that. Instead it relies on meaningless, misleading euphemisms like "program that helps conduct faster, more productive searches" and "2-3 keyword-based advertiser web pages daily".

It's easy to realize that most people simply wouldn't know what they are agreeing to by clicking through this kind of "prompt." How could they when 180 doesn't tell them in plain, straightforward language what they need to know?

I'm also struck by the assertion that 180search Assistant displays only 2-3 ads daily (a claim they repeat later in their answer to question 12). I've had 180search Assistant on my test computers—I certainly saw many more ads than that, and I only had it installed for a few hours. Maybe if you don't surf the web very much that might be true, but if you're browsing normally, you're going to get more than 2-3 ads a day.

time with a child porn browser and CoolWebSearch DirectRevenue's dirty laundry SpywareQuake scum on the run? New spyware SpywareQuake hijacking and installing malware DirectRevenue lawsuit settled Newest rogue anti-spyware installs adware from BestOffersNetwork Windows Defender Beta 2 tested against real spyware Australian press talks about Dale Begg-Smith and spyware 180solutions does it again Spyware victims can fight back Been infected with spyware? Mad about it? Tell us your story

Categories

Question 7 is important, because it returns to the issue of what 180 is doing about existing installations of its software. As I noted earlier, 180 essentially admitted to Wayne that it had "upgraded" the older nCase software on people's PCs without notifying them, even though many of those people might have gotten the software through illegal stealth-installs. Now the question becomes what is 180 doing with old versions of its 180search Assistant—pre-COAST versions, in other words, that are still being distributed by 180's distributors.

180 leads off its answer with a claim that I find absolutely blood-boiling:

> The notion that many of our users came from improper installs is an urban legend started in the anti-spyware community. Unfortunately there is a fair amount of public hysteria in the press these days about malicious software. The reality is that 80% of so-called spyware are harmless cookies.

I literally screamed when I read that. For the next few hours, this phrase kept going through my mind, "LIAR! LIAR! PANTS ON FIRE!" Now that I've calmed down a bit, let me debunk this claim as simply as possible.

Ben Edelman has documented many such stealth installations and describes them on his web pages:

180solutions Installation Methods and License Agreement

180 Talks a Big Talk, but Doesn't Deliver

Who Profits from Security Holes?

The last page above even includes a video of one stealth-install. In its white paper, Sunbelt reports that it told 180solutions that it had encountered stealth-installs of the 180search Assistant well AFTER 180 asked Sunbelt to review its software and well AFTER 180 had argued that it had cleaned up its act. One of those stealth-installs reported by Sunbelt was through a Windows Media file, an installation method that was reported on back in January:

Adware Installed through WMA Files

WMP Adware: A Case Study in Deception

Media Files that Spread Spyware

I can now report researchers at Spyware Warrior have just documented yet another stealth-install of the 180search Assistant by Wallpapers4u.com, which uses security exploits and deceptive pop-ups to install a boatload of spyware and adware on users' computers, including the 180search Assistant. This stealth-install was thoroughly documented just yesterday by Webhelper, the watcher who sees and knows all about adware and spyware vendors.

Sorry, 180. Stealth-installs of your software aren't an "urban legend." They're real, they're happening right NOW, and you know it.

180 goes further in its response to question 7, though, again attempting to give the impression that users are always clearly notified of the presence of 180's software:

> We are currently upgrading all versions of our application to reflect the changes recommended by COAST. If, after the upgrades are made, we find new installs of our

About Spyware/adware/scumware (85)
Alfred & Wendi (52)
FTC v. Spamford & Spyware (12)
General (51)
New Spyware/Adware Warnings (27)
Rogue Anti-spyware software and sites (60)
Security and Prevention (8)
Security Warnings (7)
Software Updates (85)
Spy Wiper, aka Mail Wiper, Inc., Spy Deleter (31)
Spyware Scumbags (55)
Spyware/Adware in the News (133)
The Fight (77)
Transponder Saga (3)
Weapons of Mass Spyware Destruction (26)
Webhelper Updates/Reviews (4)
Your Privacy

> older product being distributed we will turn off those applications and pursue the distributor for violation of the Code of Conduct.
>
> 180solutions provides toll-free customer support so users can contact us directly with questions and concerns about our software, installation and uninstall methods. 180solutions doesn't intend to be installed on a computer where we are unwanted, and encourage any user who feels they received our software by mistake to follow uninstall instructions.

180 then offers yet another example screenshot of a prompt window that's supposed to notify users of the presence of 180's software.

It would be nice if 180 actually displayed that notice when it's supposed to—when, say, it's upgrading older versions of its software that are still being stealth-installed by rogue distributors. But it isn't, despite the impression 180 is trying to create in this answer to Wayne's question. As it did with the "upgrades" of nCase to 180search Assistant, 180 is silently updating the software installed on people's PCs without notifying them.

"But wait!" you ask. "Shouldn't that notice prompt display when the old 180search Assistant versions update to the new COAST-certified versions from 180's servers?"

You're right. That prompt (known technically as the "CBC Force prompt") should display. But it doesn't. How is that happening? This is all explained in the Sunbelt white paper, which was yanked at 180's request. Rather than try to explain this myself, let me quote Alex Eckelberry, who still has a good description on the Sunbelt blog of what's going on:

> Here's the quick and dirty:
>
> As part of 180's COAST certification, 180 agreed to a 'CBC Force Prompt'. This feature is designed to alert users to the installation of 180's software.
>
> This prompt is shown when a certain registry key is set to '0'. If it's set to '1', there is no prompt.
>
> This is a serious weakness in the 180 installer. It is trivially easy for a rogue affiliate to simply set the value to 1, and the 180 install sails through, with the end-user none the wiser.
>
> However, it appears that 180solutions is itself electing to bypass the 'CBC Force prompt' in order to avoid alerting users to the installation of 180's software, and the implications of this are serious.
>
> Sunbelt observed several installations of older versions of the 180search Assistant in which that software was updated to the latest version. After older versions of the 180search Assistant were 'stealth-installed' via a Windows Media Player file and via a Java applet at lyricsdomain.com, that software called out to 180's servers, and downloaded and installed the latest, COAST-certified version of the 180search Assistant.
>
> This behavior is especially disturbing because many of the installations that 180solutions is silently updating through this method are the possible products of "force-installs" of 180's software of users' PCs, where those users received no notice or warning whatsoever of the 180search Assistant.

Online (5)

Spyware Help Forums

Spyware Warrior Forums
SpywareInfo Forums
Javacool Software Forums
Wilders Security Forums
Tom Coyote Forums
Cexx.org Discussion Boards
Tech Support Guy Security Forum
BroadbandReports.com Security Forum
AdAware Support Forums from Lavasoft
SpyWare BeWare
Castle Cops Security Forums
Subratam Forums
ZerosRealm Forums
Tankweb.net Forums
TeMerc Internet Countermeasures Forums

More Spyware Warriors

SpywareInfo
TeMerc Internet Security Site

> Instead of alerting users to the presence of 180's software on their systems, 180 is updating those older software installations and versions to the latest 180search Assistant, allowing 180 to continue deriving economic benefit from those installations, entirely contrary to its publicly stated intention to clean up its distribution channels.

So, rather than display the force prompt when it updates old versions of the 180search Assistant, 180 is NOT displaying the force prompt and not alerting users to the presence of 180's software on their computers, just as it did when it silently updated the old nCase software to the newer 180search Assistant.

"Is this really still happening?" you ask, incredulous. "Even after Sunbelt alerted 180 that it had found out what 180 was doing?"

The sad answer is yes, it is still happening. The same researchers at Spyware Warrior who documented the stealth-install of 180search Assistant at Wallpapers4u.com report that during that stealth-install, the version of 180search Assistant originally installed is version 5—the pre-COAST version. That old version contacts 180's servers and downloads and installs the new version 6, which should display the force prompt. But it doesn't. The version 6 just installs and continues running as before, not alerting users to the installation of 180's software.

What's especially damning is how 180 handles Wayne's question 8, which directly asks whether that force prompt is displayed when old versions of the 180search Assistant are updated to the new COAST-certified version. Wayne asked:

> 8. There are reports the new 180search Assistant has a prompt screen that displays when the software installs for the first time. But what happens when an older version of the 180search Assistant calls the 180 servers to check for updates? Will those older versions be allowed to update to the new versions? If they are allowed to update, will the new prompt screen display?

You'd think this would be the opportunity for 180 to come clean on just what is happening with that force prompt. But no. 180 completely evades the question, saying only:

> See Response to Question 7

But as we just saw, the answer to question 7 doesn't directly address the issue—it merely tries to give the roundabout, mistaken impression that the force prompt is displayed without ever directly saying it is. That's a lie by omission. The net effect of these answers is that 180solutions has lied to Wayne, lied to Sunbelt, and lied to the world about what it's doing with that force prompt.

The leopard hasn't changed its spots at all. It's still "upgrading" unwitting "users" of its software, just like it did with the old nCase installations. Only now it's trying to use those upgrades to give the impression that everything's kosher when, in fact, everything is not kosher.

Question 9: Advertising & Privacy

At times 180's answers become so tortured that it's difficult even to make sense of them. For example, in question 9 Wayne asked about 180's advertising—which 180 doesn't like to talk about, preferring instead to talk about helping users "conduct faster, more productive searches" and other such misleading nonsense. 180 responds with this:

> All advertisements displayed by 180solutions software are opened in a second browser window and presented as a Web site, rather than an advertisement.

Ben Edelman
Eric L. Howes
Doxdesk
Parasites
Tom Coyote
Counterexploitation
Patrick M. Kolla
Merijn
Javacool
WebHelper
CARMA
Alliance of Security Analysis Professionals (ASAP)
ParasiteWare.com
Wilders.org
Security Advisors
NoMoreSpyware
Scumware.com
Thiefware.com
MickeyTheMan
TomCat

Tutorials and Info

Spybot Search & Destroy Help
Spybot Search & Destroy Tutorial
HijackThis Detailed Tutorial
CoolWebSearch Chronicles
Hijack Prevention
So how did I get infected in the first place?
Spyware and other Internet Nuisances
Bleeping Computer Tutorials
Javacool

139 of 155

Huh? I defy anyone to make sense of that statement. All advertisements displayed by 180solutions software are not displayed as advertisements? What is 180 trying to say here? That they don't display advertising? But that's nonsense. And so is their answer.

180 goes on to claim that its advertising is clearly labeled, when in fact its advertising is almost indistinguishable from normal web browser windows. And, as Ben Edelman pointed out to 180solutions last summer, even the branding in the title bar that does exist may be replaced by other text if the ad page that opens is redirected. See the full discussion at ABestWeb for still more debunking by Ben of false claims made by 180 for its advertising practices.

Strangely, in its answer 180 makes a claim that its own End User License Agreement and Privacy Policy refute. 180 tells Wayne:

> There is no profiling and no capture of any browsing history.

That's just plain false. The 180search Assistant EULA flatly contradicts this statement:

> 180search Assistant will periodically direct you to our sponsors' websites. 180search Assistant will collect information about the websites you visit, but will not collect any information that will be used by 180solutions to identify you personally. The information that 180search Assistant collects and transmits to 180solutions will be used to provide you with access to comparative shopping opportunities at times when we consider them most relevant. [...]
>
> 5. Display of Advertising. The Software will collect information about you and the websites you visit ("Usage Data"), but will not collect information that will be used to identify you personally. This information will be used to provide you with comparative shopping opportunities when they are most relevant. By installing and/or using the Software you grant permission for 180solutions to periodically display sponsors' websites to you, and to collect, use and disclose the Usage Data The frequency of the advertisements will vary depending on your use of the Internet. You acknowledge that the Software includes an anonymous user ID and an electronic cookie that enables 180solutions to collect such information and to display advertising targeted to you. A "cookie" is a small amount of data that 180solutions' servers transfer to your browser and that only 180solutions' servers can read. You understand that 180solutions does not control your interaction with the web sites and advertisements displayed to you and we assume no responsibility for their content or privacy practices and policies. [...]
>
> 8. Collection of Information. 180solutions collects and uses certain information about you from your use of the Software. By installing the Software, you grant permission for 180solutions to collect this information, including the websites you visit while connected to the Internet.

180's answer to Wayne is also flatly contradicted by its own Privacy Policy:

> By installing 180search Assistant, you grant permission for 180solutions to periodically display targeted websites, to collect certain information, including the websites you visit while connected to the Internet, and to use that information as described herein. 180solutions will not use any of the information 180search Assistant collects to identify you personally.
>
> 180search Assistant. The 180search Assistant software ("180search Assistant") is a permission based search assistant application that provides access to a wide range of

Software Knowledge Base
Rogue/Suspect Anti-Spyware Products & Web Sites
Anti-Spyware Tests by Eric L. Howes
Anti-Spyware Feature Comparison by Eric L. Howes
Getting Help with Spyware
Internet Explorer Privacy & Security Settings

Blogs of Interest

VitalSecurity.org
TechDirt
SunbeltBlog
Spyware Confidential
Spyware Hunt
ResoNews
News Articles:
Business:
Wayne Porter
Flying Hamster
Security News
Technology & Marketing Law Blog
Security Fix
The Gripe Line Weblog Ed Foster
Orange Crate:

> websites, applications and information. 180search Assistant will periodically direct you to our sponsors' websites. The information that 180solutions collects under this privacy policy allows 180search Assistant to provide you with content and advertising that is targeted to your interests.
>
> What We Collect. When the 180search Assistant software is actively running on your computer, it generates logs of your web browsing activity, including web pages you have visited and the order in which you visited these pages. These logs are then uploaded to 180solutions' servers, along with an anonymous user ID assigned to the 180search Assistant software installed on your computer (your "Anonymous User ID"). We use these logs for market research purposes and to allow 180search Assistant to provide you with content specifically targeted to your interests at the time when the content is relevant. 180solutions stores these logs on our servers, for our use. We may aggregate information from these logs and share the aggregate data with third parties. The 180search Assistant software will also put a "cookie" on your machine so that we are able to recognize you and display appropriate targeted websites. A Cookie is a small amount of data that 180solutions' servers transfer to your browser and that only 180solutions' servers can read.

The profiling may be anonymous, but it is happening, and the user's browsing history is certainly being captured and uploaded to 180. Why does 180 lie like this when it has to know that its own EULA and Privacy Policy contradict what it's trying to tell people?

Questions 10-12: Wrap-up

Rather than go through the rest of 180's responses, which are mostly PR puffery and blatant nonsense, let me pick out a few claims that are demonstrably false.

In its response to Wayne's last question, 180 claims:

> It's important to note that 180solutions exceeds all standards either proposed in pending legislation or in enacted laws for downloadable applications/Internet advertising.

Wrong. HR29 (the Spy Act sponsored by Rep. Mary Bono), which was recently sent to the floor of the House and was actually passed on the floor of the House last year, has certain requirements for the notice and disclosure offered by "information collection programs" such as the 180search Assistant. Section 3.c.1.B specifies that programs like 180's software display a notice during installation:

> The notice contains one of the following statements, as applicable, or a substantially similar statement:
>
> (i) With respect to an information collection program described in subsection b.1.A: 'This program will collect and transmit information about you. Do you accept?.
>
> (ii) With respect to an information collection program described in subsection .b.1.B: 'This program will collect information about Web pages you access and will use that information to display advertising on your computer. Do you accept?
>
> (iii) With respect to an information collection program that performs the actions described in both subparagraphs (A) and (B) of subsection b.1.: 'This program will collect and transmit information about you and will collect information about Web pages you access and use that information to display advertising on your computer. Do you accept?

The Mysteryman's Chronicles
Spyware Daily
Tenebril Spyware Blog
Security Ticker

General Links

Spyware Warrior
Home PC Firewall Guide

Comment Policy & Disclaimer

All comments are the opinions of the commenter. Management takes no responsibility for the views expressed in comments.

Disclosure

In April 2005, I began doing part time consulting work for Sunbelt Software, makers of CounterSpy, as an independent contractor.

Copyright Notice

Take a look at 180's own screenshot of the notice screen for "Easy Messenger". That notice clearly doesn't fulfill HR 29's requirements, because it doesn't fully disclose all the information it needs to and uses misleading euphemisms (as I discussed earlier). If and when HR 29 does pass the full House and is enacted into law, 180solutions will be out of compliance with the federal law of the land regarding notice and disclosure for installations of spyware and adware programs.

In the same answer 180 also claims:

> The company was the first keyword search advertising provider to put an icon on the users desktop and system tray, clearly label each add, list our application in system processes, and make it simple for users to uninstall.

Again, I have to wonder why 180 makes statements that are so easily refuted. 180 is hardly the first contextual advertising company to display a tray icon for its software. Several other contextual advertising companies do this, including Claria/Gator, which has used tray icons for its applications since at least June 2002, when Ben Edelman captured the screenshot on page 1 of this PDF document.

Conclusion

Just what was 180 smoking when it compiled these responses to Wayne's straightforward questions? Who did it think it was going to deceive?

Sadly, it could very well be that 180 has successfully bamboozled some anti-spyware vendors. In response to question 11, which asked whether 180 was getting removed from anti-spyware detections, 180 claims:

> So far a handful has removed the latest versions of our applications.

Oh, really? Who might that be? Inquiring minds want to know! We know it wasn't Sunbelt. Whoever did remove these newer COAST-certified versions of 180's software simply got taken to the cleaners, that's for sure.

One final note: I have relied in part for my information on the Sunbelt white paper, which I downloaded when it was still available from the Sunbelt blog. At 180's request, Sunbelt has temporarily removed that white paper from its site. Hopefully, Sunbelt will restore that white paper, which includes plenty of information that 180 doesn't want you to know about. Now that I've seen 180's interview with Wayne Porter, I think I know why.

Update on March 5: Wayne Porter has posted a fascinating interview with the CTO of a large marketing company—about 180solutions and why many companies won't go near them now.

180solutions An Economic Interview

Said Suzi @ 8:04 pm
| Permalink | Filed under: Spyware/Adware in the News

RSS feed for comments on this post.

Comments

Unless otherwise noted, contents of this blog are Copyright © 2004 - 2006 by SpywareWarrior.com. Blog content including screenshots and videos may not be reproduced or redistributed without prior written permission.

Blog Links

RSS 2.0
Comments RSS 2.0
WP

:: Trackbacks/Pingbacks ::

1. **Wayne Porter on 180**
   To those of you following the whole "is 180 Solutions making products that deserve the adware/spwyare moniker?" debate, Wayne Porter just posted some interesting stuff on his blog. Mr. Porter, who runs a company that makes a competitor to our Counter...

   Trackback by Sunbelt Blog — 4/4/2005 7:31 am | permalink

2. **Merchants, Investors and thoughts on 180solutions**
   Wayne Porter has an opened an interesting discourse with 180solutions recently. It had been picked up by Spyware Warrior, Shawn Collins, and others. Stewardship of the internet is the heart of the matter over Zango, n-Case and other 180solutions' appl...

   Trackback by ReveNews: Beth Kirsch — 4/5/2005 11:40 am | permalink

3. [...] some decidedly questionable tactics in the past and although they claim to be clean now, not everyone is in agreeance with them. Sean Sundwall has been instr [...]

   Pingback by HTMLfixIT Web developer news. » Microsoft PR man now fights for "spyware" company — 6/2/2005 3:50 pm | permalink

:: Comments ::

1. What a load of crap. I've found 180solutions on a few computers I've cleaned up, and these people had no idea they had it. They hadn't even downloaded any "Easy Messenger."

   As far as 80% of spyware being "cookies"... I think not...I did a lady's computer about a month ago...ran Spybot Search & Destroy, and came up with 155 pieces of spyware, only a few of which were cookies. She had 180solutions, CoolWebSearch, you name it, she had it. I've seen computers with as much as 500+ pieces, but this woman had the worst ones out there, and she had no clue she had any of it.

   On a side note, what a shame this company is based out of Seattle...

   comment by Bonnie — 4/4/2005 @ 6:37 am

2. From ::scratch-a-lie-find-a-thief::
   "I've had 180search Assistant on my test computers—I certainly saw many more ads then that,"

   Do you mean "than that"? 😉

   comment by Alex — 4/4/2005 @ 7:14 am

3. Alex, I corrected the error.

comment by suzi — 4/4/2005 @ 7:27 am

4. Great summary Suzi – thanks for writing all that up, saves me the time of typing the same thing!

   I can confirm that I have observed stealth-installs of nCase (or whatever 180 want to call it) as frequently as ever over the last few months, up to and including 100%-unsolicited no-notice installation by browser security holes in pop-up ads.

   I have also observed as recently as two days ago an nCase installation loaded by IE exploit 'update' itself to the new 6.x version entirely without announcing its existence.

   If 180 really think they are effectively policing their 'affiliates' they are in cloud cuckoo land. The same sources have been using stealth installs over **years**.

   comment by And Clover — 4/4/2005 @ 10:49 am

5. What if you were wrong Suzi? Don't you realize that Ben Edelman is paid by various companies to be a critic of 180? It's the way he makes money – he is not a credible source, he's a hired gun. In fact the anti-spyware legal community held a symposium last week and purposely didnt invite him.

   comment by Jack — 4/4/2005 @ 11:22 am

6. Jack:

   Please. All of Ben Edelman's key test methodologies and results are publicly published and independently verifiable. In fact, I have examined many of Ben Edelman's claims myself and verified them, including the claims he makes about various characteristics and behavior of 180solutions' software.

   As for this business about purposely not inviting Ben Edelman to a symposium held by the "anti-spyware legal community" last week, I'm assuming you mean this one:

   http://www.law.berkeley.edu/institutes/bclt/spyware/speakers.html

   So, let's get this straight. They wouldn't invite Ben Edelman because he's a "hired gun." But they would invite Reed Freeman, "chief privacy officer" for an adware firm (Claria), and Christine Varney, who's acted as "advisor and spokesperson" for the Online Privacy Alliance (OPA)...

   http://www.privacyalliance.org/news/05121999.shtml

   The OPA, it ought to be noted, is a well-known industry front group that has no interest in protecting consumer privacy and every interest in obstructing meaningful action anywhere it might be taking place in order to protect the interests of its members, which include the likes of 180solutions, Claria, Doubleclick, and WhenU.

   With such an impressive crew in attendance, Ben Edelman ought to be honored that he was purposely not invited. Indeed, looking over the web site for that event, it's quite clear that it was simply COAST revisited—only with more lawyers.

And who, might I ask, do you represent, Jack? Please don't tell me you're a "hired gun," too, because we can only have so many of those awful people mentioned in one blog entry. (We do have our standards around here.)

And while I'm at it, Jack, just what did you think of the fact that 180 told Wayne Porter that "There is no profiling and no capture of any browsing history," when its own EULA and Privacy Policy clearly say otherwise? Does one have to be a "hired gun" to point out a lie like that?

You're going to have to do better than this, Jack.

Eric L. Howes

comment by Eric L. Howes — 4/4/2005 @ 1:31 pm

---

7. "Jack",

   Ben is not for hire; and the OPA not inviting is meaningless. Note that the OPA's members are clearly listed here.

   comment by Alex Eckelberry — 4/4/2005 @ 2:38 pm

---

8. Ben Edelman is a hired gun? Now who's smoking crack?

   Edelman, regardless of whom he is "paid by", actually documents his findings, unlike you. He doesn't just say "stealth install", he makes available a video clip of the stealth install happening. His credibility is unimpeachable. You however are just a spyware shill named Jack. If you are Jack. Liar.

   comment by Steve — 4/4/2005 @ 3:06 pm

---

9. Jack,

   I'm not a "hired gun." To the extent that I've written about 180 on my web site, this work has been without payment from anyone, and not even at anyone's request. There's no disputing that some folks then hire me to do other work—for example, to figure out how 180 is harming them and how they can make it stop. But there's no shame in this. And my work speaks for itself; I publish my methodology and my specific findings, so others can replicate my work.

   As to this past weekend's conference, it's interesting that you describe my absence as the conference "purposely [not] invit[ing]" me. How do you know? Who says so? I would think that's something only the organizers of the conference and I would know. For all the general public knows, I had other (conflicting) commitments or otherwise couldn't or didn't care to attend. I guess it would be easier to evaluate your claim if you provided some basis for it, e.g. how you know what you claim occurred.

   comment by Ben Edelman — 4/4/2005 @ 4:33 pm

10. Interesting how someone tried to turn this away from 180 Solutions and onto Ben instead. I think I have my next blog entry...!

    comment by Paperghost — 4/5/2005 @ 12:26 am

11. I'm the interviewee in Wayne Porter's follow up and have worked with Ben Edelman, unofficially, to help me clarify some of the issues in the spyware industry. I don't know who "Jack" is, but Ben Edelman is certainly above reproach. He has done nothing in my case but offer free information regarding how spyware works and how to detect it, and does this because he believes it is the right thing to do. The fact that some businesses pay him to clean up their advertising channels in no way creates a conflict of interest, and in fact he has refused my offers to further monetize his services. He is the whitest of white hats.

    comment by Jeff Doak — 4/6/2005 @ 12:54 pm

Leave a Comment

Sorry, comments are closed at this time.

Spyware Warrior

Waging the war against spyware.

4/9/2005

OH, WHAT A TANGLED WEB WE WEAVE...

On Friday CNET reporter John Borland revealed that 180solutions had bought CDT, Inc. of Mont-Royal, Quebec. 180solutions, you'll recall, has been claiming for some time that it has cleaned up its act. It's even been crowing about its admission in the now defunct Coalition of Anti-Spyware Technology vendors (COAST). True to form, 180 is spinning its latest acquisition as an opportunity to clean up its distribution channels, which are notorious for stealth-installing 180's Search Assistant software on users' computers without notifying them and getting their permission. Spinmeister Todd Sawicki of 180solutions told CNET:

> "One of the challenges with the business model in our space, where we work with distributors and affiliates, is that we don't have as much control as we like," said Todd Sawicki, director of marketing for 180Solutions. "This will give us more direct control over how our software will be downloaded."

As readers of this blog will know, I've been extremely skeptical of 180's claims for self-reform. Just last week 180 gave Wayne Porter of XBlock an interview in which they made a number of demonstrably false and misleading claims to Wayne, all of which I pointed out in my own response. So, the question is... will 180's purchase of CDT, Inc. really make that much of a difference? Will 180 finally clean up its distribution channels?

To answer that question, we need to look at some relevant facts.

Let's also watch a movie. My movie doesn't have any big name stars and it certainly won't break any records at the box office, but I think you'll find it most interesting nonetheless. Trust me.

What is CDT, Inc.?

First, there's the matter of CDT, Inc., which itself is notorious for browser hijacking and stealth installs of its BlazeFind, SearchRelevancy, WinAdClient, and WindUpdates software. See Andrew Clover's excellent write-ups on some of CDT's software at doxdesk.com:

SearchRelevancy
ISTBar

CDT has been bundling and installing 180's Search Assistant software for some time, as these several CDT license agreements disclose:

BlazeFind EULA
WinAdClient EULA
WindUpdates EULA

If you look closely at the bottom of the WinAdClient EULA, you'll notice that 180 has already started re-badging some of CDT's content.

So, 180solutions has been using CDT, Inc. to distribute its software. But CDT, Inc. has its own network of distributors, which it solicits through its LoudCash & SearchBarCash affiliate programs:

LoudCash
SearchBarCash

As you can see from the above pages, CDT pays webmasters and other software vendors to distribute its software. They are paid either on a "pay-per-install" basis or a "pay-per-impression" basis.

LoudCash has actively recruited porn webmasters to distribute CDT's software—read these two discussion threads at porn webmaster forums to see CDT's reps in action:

Need a toolbar sponsor?
New Sponsor!

And because CDT distributes 180's software, those porn webmasters could very well end up distributing the 180search Assistant. Thus we have the first few layers of the multi-level affiliate/distributor network, which Ari Schwartz of the Center for Democracy & Technology described in his recent testimony before a House sub-committee (Note: the Center for Democracy & Technology has no relationship with CDT, Inc.)

To sum it all up, this is the very kind of distribution arrangement that got 180solutions in trouble in the first place, because these pay-per-install deals effectively incentivize rogue distributors to stealth-install software on users' PCs so that they can get paid for those installs. The shrieks of users screaming at their broken, adware-infested PCs may be the sound of anguish to most people, but for CDT's LoudCash adware distributors it's "The Sound of Money."

But if that's the "sound of money," what does the "sight of money" look like? Grab some pretzels and a few cold ones, because I'm about to show you.

At Home with 180solutions & CDT, Inc.

While looking into CDT, Inc. yesterday following the announcement of its acquisition by 180solutions, I encountered a most curious web site (spazbox.net). I was surfing with the Mozilla 1.7 browser, so I wasn't that worried about getting hit with spyware or adware. Boy, did I get a surprise.

When I landed on the spazbox.net home page I immediately saw a Sun Java dialog box for a Java applet that the web site was attempting to load:

Since I see Java applets all the time at some of my favorite sites, I don't worry too much about them. I even see plenty of Java applets that have expired digital certificates, as this one at spazbox.net did. So clicked through the Java applet just as I normally do.

I should have looked more carefully at that Sun Java applet "Warning" box: the applet was from Integrated Search Technologies (IST), a well known adware vendor. Once I clicked through that "Warning" box, a whole load of adware installed without ever even offering to show me a EULA or

148 of 155

Privacy Policy. Among the programs installed were ISTBar/XXXToolbar, PowerScan, and SideFind. All of those are programs from Integrated Search Technologies, a company which is often confused with CDT, perhaps because their programs are often installed together.

But there was another program that installed—again, without showing me so much as a EULA or Privacy Policy: the 180search Assistant. What was more surprising, it turned out that the version of the 180search Assistant installed was the new version 6, which was "certified" by COAST and which is supposed to display a notice/disclosure screen (known as the "CBC Force prompt") to users. In fact, 180solutions has been telling people, such as it did in its interview with Wayne Porter last week, that this "CBC Force prompt" screen should effectively thwart rogue distributors who attempt to stealth install its software. So what happened? Why didn't I get any warning that the 180search Assistant was being installed?

As I explained in my blog entry from last week 180solutions was caught bypassing its own notice/disclosure screen when it updates old versions of its software. The technical details of how this is being done are, I admit, a bit tedious—it's all explained in last week's blog entry, though.

Rather than rehash all the boring technical details, I thought it might be more entertaining to **show** you how 180's software is being stealth-installed on PCs without displaying that CBC Force prompt. So, I went back to the spazbox.net site today. This time I took a video of the whole affair. You can download that video here:

Spazbox video

It's Showtime! 180 Stealth-Installs in Living Color!

When you watch that video, you might be overwhelmed by everything's that happening—all the boxes that pop up, all the web pages that open, etc. To help you make sense of what you're seeing, let me explain a few things.

First, most of the boxes that you see are from the firewall I was using on my test PC, Agnitum Outpost. The Outpost firewall pops up warning boxes whenever it detects "hidden processes," and you'll see boxes for a few of those. Outpost also warns when a new program on the PC is trying to access the internet, and you'll see plenty of warnings for those as well, including the 180search Assistant (named simply "Search Assistant"). Outpost also warns when an installed program with access to the internet changes in some way—perhaps as the result of an upgrade. You'll see a few of those as well, including one for the 180search Assistant, which upgrades itself from 180's servers about a third of the way through the video.

I should tell you that I specifically used the Outpost firewall so that you could see visible evidence of all the programs running and connecting out to the internet. Most users don't have firewalls, so they wouldn't see all the firewall warning boxes that I did. In fact, they wouldn't see much at all until it was far too late.

Second, let me give you a short summary of the key events in the video, so you can be watching for them.

1. As the video starts I surf to the spazbox.net web site and immediately hit a Sun Java "Warning" box for an applet from Integrated Search Technologies, which I click through. Notice that at no time am I ever told about all the programs to be installed, nor am I ever shown a EULA or Privacy Policy for any of them. There isn't even a link for me to click to get to a EULA or Privacy Policy.

Most users won't know what Integrated Search Technologies is, and they won't understand the business about the expired digital certificate either. They'll just click through the Java applet prompt as I do in the video, because there's no indication that anything's seriously wrong.

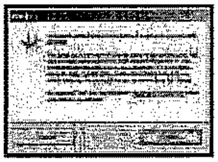
2. Very soon thereafter Agnitum Outpost begins warning that new programs are requesting access to the Internet. After a short bit, most of the adware has been installed—most of these newly installed adware programs simply want to grab more data and updates from their controlling servers. The "Search Assistant" from 180solutions is one of those programs requesting access to the internet.

3. After you see the 180search Assistant contact 180solutions' servers, start watching the system tray (next to the clock in the lower-right hand corner). If you look carefully, you'll see a new icon appear that looks like this:

That's the tray icon for the new COAST-certified version 6 of the 180search Assistant, which earlier versions didn't have. What has happened is that the version of 180search Assistant that was originally installed was version 5. It called out to 180's servers and requested any updates that were available. 180solutions' servers responded by updating the installed software to the new version 6. Once the new version 6 was installed, it added its tray icon to the system tray next to the clock.

4. Almost immediately after the tray icon appears, you'll notice that Outpost warns me that the "Search Assistant" program (sais.exe) has changed. That's because it has been updated from version 5 to version 6. I approve the change, allowing the new version 6 of the "Search Assistant" to contact 180's servers and begin downloading data files that the "Search Assistant" uses to display advertising.

So where was this "CBC Force prompt"? I don't know. It simply didn't display, even after the COAST-certified 180search Assistant was clearly installed and running on my PC. The force prompt is supposed to look something like this:



In its interview with Wayne Porter last week, 180 showed another version of the "CBC Force prompt".

So let's dig a little deeper and see what happened. I looked in the log file (sais.log) that the 180search Assistant keeps in its installation directory. This log file records all key program events as well as the user's surfing history. Below is what I found in the log file:

Notice that the log file records that the CBC Force prompt checking process was started ("CBC initialize request detected – performing CBC check"). You can also see the results of that "check": "user has already seen cbc dialog."

Did you see a "CBC Force prompt" in that installation of the 180search Assistant? No? I certainly didn't either. So the log file is just plain wrong. It says I saw the "CBC dialog" when in fact I didn't.

So, let's dig a little deeper. I checked the Registry and found the Registry flag that Sunbelt describes in its white paper (which was yanked from public view at 180's insistence.

Notice that the "cbc" Registry value is set to "1," which means that the user has already seen the "CBC Force prompt." But, again, I didn't. I got no notice that 180's software was installed on my computer, either when the original version 5 installed or when the updated version 6 installed. (And please don't tell me that the tray icon notified me—I only saw that tray icon because I knew to look for it.)

So, what we have here is a stealth-install of the 180search Assistant that works just like the Sunbelt white paper says it does. A rogue web site stealth-installed an older version of the 180search Assistant on my PC. That version "phoned home" to 180's servers and updated itself to the new version 6, which is supposed to notify the user that 180's software is installed. It didn't because 180's software set the Registry flag to "1," falsely indicating that I had seen the "CBC Force prompt" and allowing 180 to go on serving up advertising on a PC where it should never have been installed in the first place.

Call me old fashioned, but that's just plain sleazy and underhanded. No wonder 180solutions dodged Wayne's 8th question in its interview last week. In that question Wayne directly and specifically asked whether that "CBC Force prompt" would display when older versions of the "Search Assistant" updated to the new version 6.

And remember: this all is happening over 1 month after Sunbelt told 180 that it had figured out that 180 was bypassing its own notice/disclosure screen. One month after Sunbelt blew the whistle, 180 is still doing it—still bypassing its own notice/disclosure screen, allowing its software to be stealth-installed, and still lying about it.

...when first we practice to deceive.

So what are we to make of all this? Todd Sawicki claims that 180 is serious about cleaning its distribution channels, but how serious can they be if they're bypassing their own "CBC Force prompt" and telling big fat whoppers to people like Wayne Porter?

When 180 announced its admission into COAST on January 14, it promised that it would "transition to distributing only these COAST reviewed versions of its software within the next 90 days".

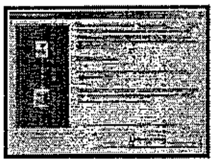
Well, folks, 180's 90 days are up come this Thursday (14 April). That's four days away. And still 180's software is being stealth-installed on people's PCs. Four days away, and still 180 is bypassing its own notice/disclosure screen when updating older versions of the 180search Assistant. Four days away, and 180 has just bought one of the most notorious hijackers and "pay-per-install" adware distributors in the business.

To top it all off, 180 says that it's buying CDT, Inc. so that it can clean up its distribution channels. I'm sorry, folks, but that just doesn't wash. The idea that 180 is cleaning up its distribution channels by acquiring CDT is a bit like believing that a drunk who buys a liquor store is solving his drinking problem because he can just order the store clerks not to sell him any more booze.

You know that won't work and I know that won't work, because ultimately it all comes down to willpower. Does 180 have the willpower? I certainly haven't seen any evidence of it. Maybe 180 thinks they're fooling people, and maybe they really have managed to fool themselves. But they haven't fooled anyone else with eyes to see what's going on.

Addendum

For the installation I reported on above, I visited spazbox.net using Mozilla 1.7. If you visit Spazbox.net with Internet Explorer, however, you'll encounter a somewhat different installation process. Instead of a Java applet from Integrated Search Technologies, you'll get hit with an ActiveX installer from CDT, Inc. that's deceptively labeled in the ActiveX "Security Warning" box as a "Website Access" program from "6247971 Canada Inc.":



If you click the link for the EULA, though, you're taken to a CDT EULA at Winadclient.com:

Although this IE-based installation process also installs the 180search Assistant, it installs a much older 5.x version than the Java-based installation process reported above does. Strangely, when that older 5.x version (from August 2004) of the "Search Assistant" updates from 180's servers, it updates only to a later 5.x version (from October 2004), not to the latest 6.x version. Why it does this is anyone's guess.

Update: Paperghost has also written about his experience with 180solutions and Java applets. http://www.vitalsecurity.org/2005/04/180-solutions-playing-with-fireand.html

Update 04-10-05: A few people mentioned it would be good to see the video of the installs from spazbox.net without the firewall alerts. Here's a second video of the installs with no interference from the firewall.

Spazbox video # 2

On a side note, in case anyone was wondering if you need a software firewall (in addition to a router), the answer is a resounding YES. The reasons should be obvious after watching both videos.

Update on 4-11-05: Many if not most of the install methods summarized here in Ben Edelman's write up Spyware Installation Methods involve 180solutions and CDT, Inc. On this page Ben specifically focuses on the involvement of 180 and CDT (Blazefind) in this deceptive, substandard installation.

Said Suzi @ 11:52 pm
| Permalink | Filed under: Spyware/Adware in the News

RSS feed for comments on this post.

Comments

:: Trackbacks/Pingbacks ::

1. **180 Solutions playing with fire...and Java applets**
   Looks like the "Java applet install of doom" is slowly working it's way across the web, as Suzi of Spywarewarrior.com has just covered yet another install using this method – however, in this case it's exploring the wonderful world of EULA-missing ...

   Trackback by Vitalsecurity.org — 4/10/2005 1:20 am | permalink

2. **Amazing blog entry by Suzi**
   Suzi at SpywareWarrior.com is one of the top spyware fighters out there.

   She posted a fascinating blog entry today.

   Trackback by Sunbelt Blog — 4/10/2005 7:07 am | permalink

3. **Lamenting the tangled web**
   Suzie, of Spyware Warrior fame, was subjected to a vicious drive-by spyware installation which included 180solutions' 180search Assistant. This from a company that says it's cleaning up its image......

   Trackback by rotas»sator — 4/11/2005 12:05 am | permalink

4. [...] ight now. We just saw installations without EULAs of adware and spyware in my write up on installs of 180solutions and other adware/spyware. So-called [...]

   Pingback by Spyware Warrior » Spyware Installation Methods — 4/12/2005 4:22 am | permalink

5. [...] f unless you know what you are doing.) Their write up includestwo videos (similar to the video I did recently on the same site), packet logs, screenhots [...]

   Pingback by Spyware Warrior » More on spazbox.net's drive by downloads — 4/12/2005 5:31 am | permalink

6. **Security guys baffled**
   I read this bit, this, and this on some serious spyware activity.

   Their question was why a domain that had no visible means of traffic building could have big alexa traffic spikes.

   After seeing what a 302 can do to traffic, I've got a little th...

   Trackback by Spam Huntress — 4/13/2005 6:32 am | permalink

7. [...] tes the Dust Spyware Installation Methods IBIS, LLC—Another Adware Company Attacking Oh, what a tangled web we [...]

   Pingback by Spyware Warrior » 2005 » April » 27 — 4/28/2005 1:59 am | permalink

:: Comments ::

1. I revisited the Lyricspy site that first carried the Java applet...sure enough, the Sais.log value had been apparently fiddled with there too. Stealth installs galore!

   comment by Paperghost — 4/10/2005 @ 12:59 am

2. Note also that the IST installs (as was as CDT's own) are still both being triggered from CoolWebSearch browser security holes exploits. These exploits add IST, CDT and others to the Trusted Zones and/or Trusted Publishers lists, and then open IE on one of their download pages so the software downloads straight away without warning.

   So you don't even need to click 'Yes' to a Java or ActiveX download box.

   This is just one of the ways 180 software has been distributed for months (years, even) without any kind of consent.

   comment by And Clover — 4/10/2005 @ 4:44 am

3. I hate hearing about this stuff. Hardly gives us hope for ever having a safe environment to play in...

   I turned off Java in Firefox a while back for just this kind of thing. I've got to admit that I really don't miss it too much. 🙂

   comment by Steve D — 4/10/2005 @ 11:11 pm

4. incredible video clip indeed, i was blown away by what i saw!
   wow, what an experience

   comment by Shri — 4/17/2005 @ 7:48 pm

5. I'd like to be able to file suit against the spyware vendors under the Virginia Consumer Protection Act (specifically, Va. Code sxn 59.1-200(14) and 59.1-204, which provides for $1,500 statutory damages for deceptive conduct). And, being an attorney, it's pretty easy for me to do that. But I have trouble finding sufficient info on CDT, Inc. and 180 etc. to be able to properly name the defendants. Can you help with that?

   comment by dlh — 5/13/2005 @ 2:57 pm

6. The gall of the distributors to Presume that WE want and will Tolerate any recording device on OUR computers, is Sheer Folly!! To think that a Complete Stranger no matter Who they Are would think WE would let them "listen" on our computer and find out where we surf to and what we type. I DON'T want Crooks like them who you CAN'T Trust on my Computer. You Never Know WHO their going to give YOUR Personal info to!! My own Mother is aghast at what their doing and she says she is Glad she Doesn't have a computer!!! I'm almost wishing that I could throw my computer out the window! Alas you Can find Protection on the Computer that is Free and doesn't cost an arm and a leg!
   Important: I'm happy I don't have Gator on my computer, but I've found it a few times in the Registry and Always deleted it. From now on, I'll keep looking in the Reg. Finally I know what software to use to keep it out of my computer. I've got to buy XBlock soon...Thank you.

   comment by Julie — 6/20/2005 @ 8:19 pm

Leave a Comment

Sorry, comments are closed at this time.